ESCOLA NAVAL

Talant de bien faire

Catarina de Sousa Matos Aresta

Resilience of the PNT Systems

A Portuguese Case Study

Dissertação para obtenção do grau de Mestre em Ciências Militares Navais, na especialidade de Marinha

Alfeite
2017

Catarina de Sousa Matos Aresta

Resilience of the PNT Systems
A Portuguese Case Study

Dissertação para obtenção do grau de Mestre em Ciências Militares Navais, na especialidade de Marinha

Orientação de: CFR Plácido da Conceição

O Aluno Mestrando

O Orientador

____
[nome]

____
[nome]

Alfeite

2017

"Resilience is very different than being numb. Resilience means you experience, you feel, you fail, you hurt. You fall. But, you keep going."

Yasmin Mogahed

To my family for their support but, in a more special way, to my sister Rita for being an example of eloquence, brilliance and persistency.

Acknowledgements

Firstly, I would like to thank my Thesis Supervisor, Commander Plácido da Conceição, for guiding me throughout the whole research process, always keeping me motivated and interested in finding out more about this theme.

Secondly, I would like to thank Lieutenant Commander Figaldo Neves, for offering me help throughout the technical and experimental aspects of my study.

Thirdly, but just as important, I would like to thank all the Organisations and participants that helped me throughout this project: Gabinete Nacional de Segurança, Direção Geral do Território, Autoridade Marítima Nacional, Centro de Informação Geoespacial do Exército, Portuguese Air Force, Svitzer, Faculdade de Ciências da Universidade de Lisboa, GMV, Vessel Traffic Service, Comando Naval for providing a naval unit for my experiment, Centro Integrado de Treino e Avaliação Naval, Centro de Comunicações Dados e Cifra da Marinha, Esquadrilha de Submarinos, Esquadrilha de Helicópteros, NRP *D. Francisco de Almeida*, NRP *Bartolomeu Dias*, NRP *António Enes*, NRP *Arpão*, Direção de Navios and Instituto Hidrográfico.

x

x

Abstract

There is a high national dependency on Position, Navigation and Timing (PNT) Systems for several individuals, services and organisations that depend on this information on a daily basis. Those who rely on precise, accurate and continuous information need to have resilient systems in order to be highly efficient and reliable. A resilient structure and constantly available systems makes it easier to predict a threat or rapidly recover in a hazardous environment.

One of these organisations is the Portuguese Navy, whose main purposes are to combat and maintain maritime safety. In combat, resilient PNT systems are needed for providing robustness in case of any threat or even a simple occasional system failure. In order to guarantee maritime safety, for example in Search and Rescue Missions, the need of PNT information is constant and indispensable for positioning control.

The large diversity of PNT-dependent equipment, developed over the last two decades, is a valid showcase for the high GPS dependency that is seen nowadays – which is vulnerable to various factors like interference, jamming, spoofing and ionospheric conditions. The recent interest over integrated PNT system resolutions is related to the search for redundancy, accuracy, precision, availability, low cost, coverage, reliability and continuity.

This study aimed to build a current PNT Portuguese picture based on Stakeholder Analysis and Interviews; assess the vulnerability of those who depend mainly on GPS for PNT information and, find out what the next steps should be in order to create a National PNT Strategy.

Key-words: Resilience, PNT, GNSS, Stakeholders, Vulnerability.

Resumo

Existe uma elevada dependência nacional em sistemas de Posição, Navegação e Tempo (PNT) por parte de diversos indivíduos, serviços e organizações que dependem desta informação no seu dia-a-dia.

Todos os que dependem de informação precisa, exata e contínua, necessitam de ter sistemas resilientes para que sejam altamente eficientes e fiáveis. Uma estrutura resiliente e sistemas continuamente disponíveis facilitam a previsão de possíveis ameaças ou a expedita recuperação da funcionalidade, em ambientes hostis.

Uma destas organizações é a Marinha Portuguesa cujas funções principais são o combate, a salvaguarda da vida humana no mar e a segurança marítima e da navegação. Para o combate, são necessários sistemas PNT, resilientes, que ofereçam robustez em caso de uma simples ameaça ou falha temporária dos sistemas. Por forma a ser possível cumprir a missão, a necessidade de ter informação PNT, fidedigna e atualizada, é constante e indispensável para o controlo preciso e exato da posição. Uma unidade naval, por forma a permanecer continuamente no mar, manter a sua prontidão, treinar a sua guarnição ou ser empenhada num cenário de guerra, necessita de saber, com confiança e sem erros, a sua posição e referência de tempo.

A grande diversidade de sistemas dependentes de informação PNT, desenvolveu-se em larga escala nas últimas duas décadas e sustenta cada vez mais a alta dependência do GPS, que é vulnerável a diversas fontes de erro, tais como interferência*,* empastelamento*,* mistificação e condições ionosféricas. Atualmente, o elevado interesse na criação de sistemas PNT integrados está associado à procura da redundância, exatidão, precisão, disponibilidade, baixo custo, cobertura, fiabilidade e continuidade.

Este estudo teve como objetivos construir o panorama atual, em Portugal, ao nível dos Sistemas PNT, baseando-se numa análise de *Stakeholders* e entrevistas; avaliar a vulnerabilidade de organizações e serviços que dependam exclusivamente do GPS como fonte de informação PNT; e propor um possível caminho para que seja possível criar uma Estratégia PNT Nacional.

Palavras-chave: Resiliência; PNT; GNSS; Stakeholders; Vulnerabilidade.

Contents

List of figures

List of Tables

List of Abbreviations and Acronyms

AAPS – *Automatic Identification System Autonomous Positioning System*

AIS – *Automatic Identification System*

APNT – *Alternative Position, Navigation and Timing*

ASF - Additional Secondary Factor

AtoN – *Aids-to-Navigation*

BDS – *BeiDou Navigation Satellite System*

C/A-code – *Coarse/Acquisition code*

CDMA – *Code Division Multiple Access*

CRPA - *Controlled Radiation Pattern Antennas*

CSAC – *Chip scale atomic clock*

C-SCAN - *Chip-Scale Combinatorial Atomic Navigator*

DARPA - *Defense Advanced Research Projects Agency*

DASS – *Distress-alerting Satellite System*

DCS – *Data Coding Scheme*

DGPS – *Differential Global Positioning System*

DME – *Distance Measuring Equipment*

DSC - *Digital Selective Calling*

EDTR – *e-LORAN Differential Time Receiver*

EGNOS – *European Geostationary Navigation Overlay System*

e-LORAN – *enhanced-long range navigation*

ESA – *European Space Agency*

EU – *European Union*

EUROCONTROL – *European Air Traffic Control*

FDMA – *Frequency Division Multiple Access*

GAGAN – *GPS-Aided GEO Navigation System*

GAARDIAN - *GNSS Availability Accuracy Reliability and Integrity Assessment for timing and Navigation*

GAUL - *Galileo Assist Using e-LORAN*

GBT – *Ground Based Transceiver*

GEO - *Geostationary*

GLA - *The General Lighthouse Authorities of the United Kingdom and Ireland*

GLONASS – *Globalnaya Navigatsionnaya Sputnikovaya Sistema (Global Navigation Satellite System)*

GMDSS – Global Maritime Distress Safety System

GNSS – *Global Navigation Satellite System*

GPS – *Global Positioning System*

GPSS – *Global Positioning system-of-systems*

GSM - *Global System for Mobile Communications*

HRO - *High-Reliability Organisation*

ID – *Investigation and Development*

IMO – *International Maritime Organization*

IMU – *Inertial Measurement Unit*

INS – *Inertial Navigation System*

IRSS – *Indian Regional Satellite System*

ISRO – *Indian Space Research Organization*

ITU – *International Telecommunications Union*

LDC – *Loran Data Channel*

LF – *Low-Frequency*

MCC – *Mission Control Centres*

MEO – *Medium Earth Orbit*

MF – *Medium-frequency*

MSAS – *Multi-functional Satellite Augmentation System*

NATO – *North Atlantic Treaty Organization*

NDGPS – *National Differential Positioning System*

NLES – *Navigation Land Earth Stations*

NMEA - *National Marine Electronics Association*

NTP – *Network Time Protocol*

P-code – *Precision code*

PDU - *Power Distribution Unit*

PHM - *Passive Hydrogen Maser*

PNT – *Position, Navigation and Timing*

PPS - *Precise Positioning Service*

PRN – *Pseudo Random Noise*

QZSS – *Quasi-Zenith Satellite System*

RAFS - *Rubidium Atomic Frequency Standard*

RAIM - *Receiver Autonomous Integrity Monitoring*

RIMS – *Ranging and Integrity Monitoring Stations*

RF – *Radio Frequency*

RNSS – *Regional Navigation Satellite System*

RTK – *Real Time Kinematics*

SAASM - *Selective Availability Anti-Spoofing Module*

SBAS – *Space-based Augmentation System*

SDCM – *System for Differential Corrections and Monitoring*

SENTINEL - *GNSS Services Needing Trust in Navigation, Electronics, Location & Timing*

SIS – *Signal-in-space*

SNR - *Signal-to-Noise Ratio*

SOP – *Standard Operational Procedures*

STAMP - *Systems-Theoretic Accident Modelling and Processes*

SPS - *Standard Positioning Service*

TAI - *International Atomic Time*

TOA – *Time of Arrival*

UK – *United Kingdom*

UPS - *Uninterruptible Power Supply*

U.S. – *United States*

USA – *United States of America*

UTC – *Coordinated Universal Time*

VHF – *Very High Frequency*

VTS - *Vessel Traffic Service*

WAAS – *Wide Area Augmentation System*

WAGE – *Wide Area GPS Enhancement*

WARTK – *Wide Area Real Time Kinematics*

Introduction

What would we do if suddenly our positioning and timing satellites were instantly turned off? Most things we do on a daily basis use Global Navigation Satellite Systems (GNSS) as a position, navigation or time reference: ships, aircrafts, cars, electricity distribution companies, national defence departments and even citizens. "Over 130,000 manufacturing jobs and over 3 million people are involved in some aspect of the downstream GNSS markets for their livelihoods. The commercial value of the direct and indirect markets are difficult to precisely define, but is in the range of US$100 billion per year in the United States alone. Worldwide it exceeds $175 billion."[1]

The Global Positioning System (GPS), one of the mostly used PNT systems of nowadays, is almost the only available option for civil and military marine navigation in most countries. However, this system is very vulnerable to ionospheric[2] or accidental interference[3], jamming or spoofing[4]. This leaves warships only with few or no alternatives to assure continuous PNT information. Without this information or if it is not precise, a warship will not be able to know its position and time reference in a war scenario or rescue mission, in an swift manner.

Over the last decade, large developments have been made in the jamming equipment market, which made buying these cheap gadgets online easier. This means that one could easily compromise the maritime safety[5] and, consequently, the Safety of

[1] Scott Madry, *Global Navigation Satellite Systems and their Applications*, New York, Springer Science + Business Media LCC, 2015, p 2.

[2] Paul Kintner, Todd Humphreys, Joanna Hinks, "GNSS and Ionospheric Scintillation", *Inside GNSS*, July/August Issue, 2009, http://www.insidegnss.com/node/1579, (accessed April 2017).

[3] Andrew Dempster, *Boaters beware GPS vulnerable to interference and jamming*, 2016, http://www.marinebusinessworld.com/n/Boaters-beware-GPS-vulnerable-to-interference-and-jamming/81275?source=google.pt, (accessed April 2017).

[4] Joe Uchill, *Why GPS is more vulnerable than ever*, http://projects.csmonitor.com/gps, (accessed April 2017).

[5] Alan Grant, *et al.*, *Understanding GNSS availability and how it impacts maritime safety*, San Diego, The General Authorities of the United Kingdom and Ireland, 2011.

Life at Sea by locally denying the use of GPS signals. Under these circumstances, the need for redundancy and creating new PNT alternatives was intensified. The International Maritime Organisation's (IMO) strategy for the e-Navigation adoption[6] states that before developing the Electronic Navigation area, a new robust, redundant positioning system must be adopted, only initially due to its vulnerabilities – using GNSS. Organisations that depend on continuous and reliable PNT information need to be equipped with resilient and robust systems.

The Portuguese Navy, on which this study mostly focuses on, needs to be provided with accurate PNT information in order to operate far from harbours and coastlines, it is a High Reliability Organisation (HRO)[7] and its missions include military defence in normal or hazardous conditions, Search and Rescue operations and provision of maritime navigation safety services.

With the intent of contributing to a current perspective of the Portuguese PNT dependency and, more specifically, the Portuguese Navy, this study is based on two convergent lines of investigation. The first part of the investigation consisted in collecting data on the current Portuguese PNT picture by interviewing, through a questionnaire and personal interview, the PNT stakeholders. The second part consisted of submitting a Portuguese Navy naval unit to a GPS-denied environment to make an assessment on its dependency and decision-making upon an uncommon and unexpected scenario.

Objectives

The central question of this project is: "Why should PNT systems be resilient?" Secondary questions are then derived from the main question:

- How can a PNT system be resilient?
- What are the Portuguese PNT stakeholders looking for in a PNT system?
- What is the current perspective of PNT systems in Portugal?

---

6 Sub-Committee on the Safety of Navigation, *Development of an E-Navigation Strategy Implementation Plan*, United Kingdom, International Maritime Organisation, 2011, pp 18-25.

7 Daved Stralen, *High Reliability Organisations*, High Reliability Organizing, http://high-reliability.org/High-Reliability-Organisations, (accessed April 2017).

- How are the Portuguese Warships vulnerable to (un)intentional GPS information denial?

This research starts with a theoretical approach to this theme, including the definition of resilience and PNT systems. This is followed by clarifications on the requirements for a resilient PNT System.

The merging of these theoretical concepts with the study about the PNT systems that are currently available in Portugal and more specifically aboard Portuguese Warships, it was possible to build a perspective of the Portuguese PNT current picture; to know what the stakeholders look for in PNT system; to investigate if there is national resilience awareness and at last but not least, to investigate how Portuguese Warships are vulnerable to intentional or unintentional GPS denial.

Methodology

This study began with a bibliographic research of articles, publications and books related to the concepts of resilience; Position, Navigation and Timing Systems and in which way are they considered resilient.

Then, an initial stakeholder analysis was made to identify attentive Portuguese GNSS Stakeholders. This process was guided by a previous study[8] led by RAND Corporation, who develops research and analysis for the United States (US) Department of Defense. This study includes a description of the US' GPS Stakeholders which facilitated the process of determining the Portuguese GNSS stakeholders.

After the stakeholder analysis process, an online questionnaire and open-ended interview with the stakeholders was performed, to collect data from those who were considered illustrative for a national representative picture. The sampling method that was used for the Stakeholders selection was the *non-probabilistic method*[9] which means that each of them were selected based on previously chosen criteria and known

---

[8] Scott Pace, *et al*., *The Global Positioning System: Assessing National Policies*, California, RAND Corporation, 1995, pp 11-44.

[9] Hermano Carmo, Manuela Ferreira, *Metodologia da Investigação, Guia da Auto-aprendizagem*, 2ª Edição, Lisboa, Universidade Aberta, 2008, pp 209-210.

probability is not guaranteed. The non-probabilistic method used was the *typical case sampling*[10] due to time limitations and also because the interviewees are intentionally chosen due to sharing a common element. In this process of sampling, unique or special cases may be included to bring authenticity to the study.

The online questionnaire was created based on closed questioning[11], using control questions[12] and also using the *Likert scale*[13]. The software used was the open-source software Google Forms. The interview type used was dominantly formal – an interview with open questions[14] to focus mostly on the interviewee's knowledge. Both of the stakeholder data collection methods: Inquiry by interview and Inquiry by questionnaire have pros and cons. As a result, the information obtained makes both of these methods complement each other.[15] The whole process made it possible to find out what the Portuguese GNSS stakeholders look for in a PNT system and also to construct an updated picture of the PNT development in Portugal.

Finally, a GPS Jamming Trial was performed, using physical equipment to collect GPS data and, also, to analyse the crew's reaction when bound to a hostile environment. Several guidelines were used to conduct a Case Study with Field Observations[16], such as prevision; first sight; additional preparation for the observation; additional conceptualisation for the development; data collection and validation; data analysis and, eventually, give the public a comprehension opportunity.[17] This last aspect, made it

[10] Hermano Carmo, Manuela Ferreira, p 216.

[11] *Ibidem*, p 157.

[12] *Ibidem*, p 158

[13] *Ibidem*, p 160.

[14] *Ibidem*, pp 146-148.

[15] *Ibidem*, p 164.

[16] Robert Stake, *A Arte de Investigação com Estudos de Caso*, Tradução de Ana Maria Chaves, Lisboa, Fundação Calouste Gulbenkian, 2007, pp 68-70.

[17] Ibidem, p 68-70.

possible to test whether the Portuguese Warships are prepared in the event of an unexpected scenario.

Structure

This dissertation consists of an introduction, five content chapters and a discussion.

- **Introduction**. Includes a brief description of the context, objectives, methodology and structure of the dissertation.
- **Chapter 1 – What are resilient PNT Systems?** This chapter starts by defining resilience, followed by a definition of PNT Systems and how they can be resilient. Then, there is a brief explanation of PNT systems that are available or under development.
- **Chapter 2 – GNSS Vulnerabilities.** This chapter portrays the vulnerabilities that these systems are sensible to: interference, jamming and spoofing, among others. Previous jamming and spoofing trials performed by other countries are also laid out in this chapter.
- **Chapter 3 – Study Methodology.** This chapter explains the adopted methods, namely for the process of data collection, results presentation and analysis.
- **Chapter 4 – Results.** This chapter presents all the data acquired in the online questionnaire/personal interviews and also the data collected in the Jamming Trial.
- **Chapter 5 – Analysis.** This chapter comprises the discussions that were made after processing the collected data.
- **Chapter 6 – The Path for a Resilient PNT System in Portugal.** This chapter shows an updated Portuguese PNT picture and advises the measures that should be taken by Portugal and the Portuguese Navy.
- **Conclusion.** This chapter shows a brief explanation of how the results were obtained; the difficulties faced in data collection and improvements that could have been made. A final suggestion for a future project is also presented.

Chapter 1 – What are resilient PNT Systems?

1.1 What is Resilience?

"Resilience is a property intimately associated with the organisations' capacity to avoid, contain and mitigate accidents."[18] When it comes to having a resilient system, it means it can deal with unexpected events or failures and catastrophes. Resilience cannot be classified as a technical or organisational mean - if an organisation operates resilient systems, then it is resilient too. Both concepts can be and are related.

Having a resilient system does not mean that it absolutely cannot fail – it means that it somehow has a way to be back online by itself when submitted to a vulnerable situation. This leads to the fact that a resilient system must instate both technology and its operators but also be robust[19], flexible[20], redundant[21], available[22], precise[23], accurate[24] and continuous[25].

Pedro Antunes and Hernâni Mourão, in their Resilient Business Project Management Report described five key aspects that support system resilience, such as:

---

[18]Pedro Antunes, Hernâni Mourão, *Resilient Business Process Management*; *Frameworks and Services*, Lisbon, Faculdade de Ciências da Universidade de Lisboa, 2011, p 2.

[19]*Ibidem*, p 5.

[20]*Ibidem*, p 5.

[21]International Maritime Organization (IMO), *Resolution A.915 (22)*, *Revised Maritime Policy and Requirements for a Global Navigation Satellite System*, IMO, 2001. p 9.

[22]*Ibidem*, p 6.

[23]*Ibidem* p 8.

[24]*Ibidem*, p 6.

[25]*Ibidem*, p 6.

- Failure handling – "systems operate in heterogeneous, distributed and autonomous platforms that are prone to component, communication and system failures"[26];
- Exception handling – "Unlike failures, which result from system malfunctions, exceptions come from semantic discrepancies between the actual organisational environment and the processes modelled by the system"[27];
- Model adaption - due to "incomplete developments, development errors and changes in the business environment"[28];
- Restricted *Ad-hoc* changes – "concern operations not predicted in the process models and carried out during the execution phase to accomplish work"[29];
- Unstructured interventions - it should be already predicted that "cascading"[30] events might occur. The concept "cascading" can be defined as "to occur in a sequence or successive stages"[31]. In this case, it means events that consequently lead to the occurrence of others successively and without warning. This may lead to a chaotic situation.

For GNSS, Alan Cameron believes that resilience goes way "beyond what we normally think of as position and timing sensors"[32]. Cameron also gives us the concept that PNT is much more than sensors complementing each other. It is more of a mixture of

[26]Pedro Antunes, Hernâni Mourão, p 6.

[27]*Ibidem,* p 7.

[28]*Ibidem*, p 8.

[29]*Ibidem*, p 8.

[30]*Ibidem*, p 9.

[31]The Free Dictionary by Farlex, http://www.thefreedictionary.com/cascading, (accessed on May 2017).

[32]Alan Cameron, "Resilient", *GPS WORLD*, January Issue, 2016, p 6.

hardware and software, old and new data coming from sources that we do not even regard as PNT sources. These sources could even be amateur applications.[33]

So how is it possible to monitor resilience? Firstly, there is a need to evaluate whether and how do the systems adapt to different kinds of derangements. Rojier Woltjer claims that to monitor resilience the following properties should be considered:

- Buffering capacity – "the size or kind of disruptions the system can absorb or adapt to without a fundamental breakdown in performance"[34];
- Flexibility - "the system's ability to restructure itself in response to external changes or pressures"[35];
- The margin – "how closely or how precarious the system is currently operating relative to one or another kind of performance boundary"[36];
- Tolerance - "how a system behaves near a boundary"[37], for instance if it loses information quality or simple blacks-out;
- Cross-scale interactions – "the resilience of a system defined at one scale depends on influences from scales above and below"[38].

In order to be a High Reliability Organisation (HRO) – such as aviation and air traffic companies, space exploration organisations, nuclear power plants – an organisation needs to have resilient systems in order to be prepared for "blackouts", system failure and to quickly be back online. Why then, should the Portuguese Navy be a HRO? Firstly, a HRO manages to keep going with their production and offer high reliability when submitted to precarious, risky or calamitous conditions, without disturbing human lives due to the designed and developed combination of men and technology, and

[33]Alan Cameron, "Resilient", p 6.

[34]Erik Hollnagel, David Woods, Nancy Leveson, *Resilience Engineering*, *Concepts and Precepts*, Aldershot, Ashgate Publishing Limited, 2006, p 23.

[35]*Ibidem*, p 23.

[36]*Ibidem*, p 23.

[37]*Ibidem*, p 23.

[38]*Ibidem*, p 23.

perpetuating the financial and environmental conditions. The Portuguese Navy should, then, be a HRO as its main mission involves military operations that require fast and effective responses and also taking responsibility in keeping maritime security. Operations that involve saving human lives or dealing with dynamic, unpredictable and complex operational contexts require a flexible and adaptive organisation with robust and resilient systems that have the capability to react and keep going among unpredicted failures.

System resilience leads us to the concept of resilience engineering. David Woods considers four leading concepts for resilience[39] in resilience engineering:

- “Rebound from trauma and return to equilibrium”;
- “Synonym for robustness”;
- “Opposite of brittleness”;
- “Network architectures that can sustain the ability to adapt to future surprises as conditions evolve”.

Woods also states that we are facing a technological problem nowadays, due to interconnected networks of several systems that, when put to a single system failure, may cause the whole network to be disrupted. This is why, in the last decade, a whole new effort has been put into this concept of resilience. “The empirical progress has come from finding, studying, and modelling the biological and human systems that are prepared to handle surprises.”

As technology and society are in constant change and development, in order to create a resilient system capable to respond to any kind of event, risk management cannot be ignored and needs to be proactive. “Risk management in the present context is directed towards control of the risk related to the dynamic course of events following a disturbance of a potentially hazardous physical process.” Rasmussen claims that there is a high risk in technology manufacturing, in the present, due to the fact that organisations and companies are combining ancient management techniques with ultra-modern

---

[39]David Woods, *Four concepts for resilience and the implications for the future of resilience engineering*, Columbus, The Ohio State University, 2015, p 1.

technology. For that reason, in order to perform a proactive risk management analysis when developing a resilient and prosperous system, there are several types of accidents with different risk management strategies[40]:

- Occupational safety – when a small but frequent accident occurs and is controlled based on past accidents (empirical);
- Medium-sized accidents – lead to design improvement, as they are not so frequent. Risk management is normally achieved by removing the accident causes;
- Large-scale accidents – as they have a very low probability of occurring, risk management cannot be empirical. This means a probabilistic analysis has to be made in order to identify what events are mostly probable to occur and identify their causes in order to remove them or upgrade the separate systems to more resilient ones.

A resilient organisation must have safety as a key-value, because safety is reflected on the failures that do not actually occur. One of the biggest flaws related to resilience happens when a system seems resilient, and research and development tend to decrease, as well as investment and maintenance budgets. The fact is, technology keeps changing as well as unpredicted flaws may occur.

1.2 The path to PNT

1.2.1 Looking through GNSS

The United States were the first in developing one of the position and timing reference systems and, in fact, the most commonly used one: the Global Positioning System (GPS), a space-based radionavigation system. After the United States, some interested countries started developing their own GNSS. Russia started developing

[40]Jens Rasmussen, Inge Svedung, pp 27-28.

GLONASS in the late 70s[41], the European Union (EU) started developing GALILEO in 1999[42]. China more recently started developing BeiDou II Navigation Satellite System (BDS), which aims to be totally launched by 2020[43]. Japan and India also started developing their Regional Navigation Satellite Systems (RNSS): Quasi-Zenith Satellite System (QZSS) and the Indian Regional Navigation Satellite System (IRNSS), correspondingly. These countries are trying to work on GNSS resiliency (by creating their own satellite systems for redundancy) but not through offering a full solution as these systems work based on a GPS-like technology with weak satellite signals, only operating in different compatible frequencies.

As we know, GPS can offer accurate PNT information and is still the military's leading system. However, the information is not always available or reliable, but it is still used by several ships' equipment, as it can be seen in Figure 1, apart from the Global Maritime Distress Safety System (GMDSS) that is also GPS-dependent and is missing in Figure 1. If GPS by any chance fails, the actual equipment, or any other equipment that depends on its information, fails to offer accurate data or any data at all.

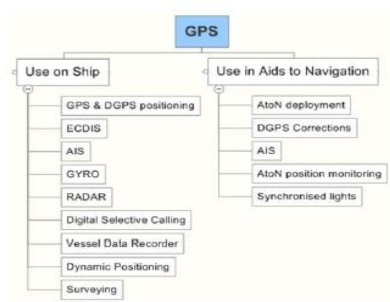


Figure 1 - Ships' equipment using GPS[44]

[41] Scott Madry, *Global Navigation Satellite Systems and their Applications*, New York, Springer Science + Business Media LCC, 2015, p 45.

[42] Vincent Reillon*, Briefing GALILEO: Overcoming obstacles, History of EU Global Navigation Systems*, 2017, p 6.

[43] Shau-Shiun Jan, An-Lin Tao, *Comprehensive Comparisons of Satellite Data, Signals, and Measurements between the BeiDou Navigation Satellite System and the Global Positioning System*, National Cheng Kung University, Taiwan, 2016, p 1.

[44] Paul Williams, Chris Hargreaves, "UK eLoran – Initial Operational Capability at the Port of Dover", *Proceedings of the 2013 International Technical Meeting of The Institute of Navigation*, California, 2013, p 393.

GPS, in order to be constantly reliable and available, needs a software and hardware redesign to be able to rapidly include or exclude different sensors and it should also be compatible with all civilian and military needs.

How does GPS then work? It works by comparing the different signals with the same codes that are broadcasted from each satellite and processing the timing difference between them. Nowadays, normally at least four satellites are in view, and in that manner, a more rigorous position can be determined, as the fourth satellite is essential for a 3D position. With the intersection of four spheres, there is only one place in the world where you can be at.[45] However, if only three satellites are visible, a position still can be determined making the assumption that the receiver is at the mean sea level.[46]

How can timing be so accurate, then? Each GPS satellite possesses incorporated caesium and rubidium atomic clocks. For example, a caesium atomic clock works by electrifying caesium atoms with microwave energy until they start vibrating. A caesium atom has a frequency of 9,192,631,770 Hz[47], the frequency of the vibration is then measured and, it is used as a timing reference. "The second itself was defined by the caesium atomic clock method in 1967, and it was in 1971 that International Atomic Time (TAI) was defined"[48].

In order to compute the exact time, it would be much simpler if each GPS receiver possessed an atomic clock itself but, that, would be make each unit much more expensive, so the receiver actually seizes the signals from minimum three satellites - for a two-dimensional position and minimum four satellites for a three-dimensional position - in view, processes the signal codes and measures its own clock error. This time will be the one that the receiver will adopt. This process is a repetitive cycle.

---

[45]Scott Madry, pp 35-40.

[46]Integrated Mapping Ltd., *How GPS Works*, https://www.maptoaster.com/maptoaster-topo-nz/articles/how-gps-works/how-gps-works.html, (accessed May 2017).

[47]United States Naval Observatory, *Cesium Atoms at Work*, http://tycho.usno.navy.mil/caesium.html, (accessed October 2016).

[48]Scott Madry, p 35.

The GPS System provides two types of service: the Standard Positioning Service (SPS) and the Precise Positioning Service (PPS), conceived for authorised military users.[49]

The PPS uses both L1 (1575.42 MHz)[50] and L2 (1227.60 MHz)[51] frequencies. The L1 and L2 frequencies contain a coarse/acquisition code (C/A-code) that is available for all civil, commercial and military receivers and a Precision code (P-code) only for authorised users. The P-code is cryptographically altered to become the Y-code and is not available to those who do not have the cryptographic keys.[52] The performance levels using the C/A-code receivers are 5 – 10m accuracy, and using the P/Y-code receivers, 2 – 9 m.[53]

A new GPS generation is in development as "in 2014 Lockheed-Martin won the contract for the new Block III satellites that will have a second civilian code, improved anti-jamming capabilities, a stronger signal, more power, a new military code, and a completely upgraded ground control segment."[54]

Several systems have been created, since the development of GPS, to upgrade the nature and accuracy of many civilian positioning systems. The Differential GPS, or DGPS, uses various reliable fixed stations with known positions, which are compared to the received GPS signal. The difference between these two positions is transmitted in almost real time, constantly, by Low-Frequency (LF) radio waves to the surrounding GPS receivers. Our position can be obtained then with a 0.7 – 3m accuracy (in C/A-code) and 0.5 – 2m (in P/Y-code)[55]. A considerable difference between DGPS and GPS is that, DGPS,

---

[49]Fisheries and Oceans Canada Coast Guard, *Primer or GPS and DGPS,* Canadian Coast Guard, 2000, p 7.

[50]European Space Agency Navipedia, *GPS Signal Plan*, 2011, http://www.navipedia.net/index.php/GPS_Signal_Plan, (accessed June 2017).

[51]*Ibidem*.

[52]European Space Agency Navipedia, *GPS Services*, 2011, http://www.navipedia.net/index.php/GPS_Services, (accessed June 2017).

[53]European Space Agency Navipedia, *GPS Performances*, 2011, http://www.navipedia.net/index.php/GPS_Performances, (accessed June 2017).

[54]Scott Madry, p 43.

[55]European Space Agency Navipedia, GPS Performances.

can send warnings to the users in case the system is unreliable (integrity monitoring)[56]. In Portugal, there are currently four operational DGPS stations (Cabo Carvoeiro, Sagres, Horta and Porto Santo) and a monitoring station in the *Direção de Faróis* (Paço de Arcos)[57]. Despite the fact that ground-based rectification systems using DGPS are very useful, they have the same vulnerabilities as GPS.

For this matter, Ground Based Augmentation Systems (GBAS) were created to enhance GPS' precision.[58]This system is of indispensable use in precision landings and approaches. A GBAS Ground Facility consists, normally, of three GPS antennas, a processing utility and VHF Data Broadcast transmitter. A user, in order to operate this system, should have a Very High Frequency (VHF) Antenna.[59] The GPS antennas that the GBAS beholds are in known positions. The receivers measure the time that the signal takes to travel from the GPS satellites to the antennas and calculate the distance. This calculated distance is then compared to the actual known distance in order to determine the error.[60] The GBAS Ground address has the capability to monitor the performance of the GPS satellites which makes it possible to stop receiving signals from a certain satellite if that its information is considered unhealthy.[61] Space-Based Augmentation systems (SBAS) have also been established and consist of:

> "A ground infrastructure that includes the accurately-surveyed sensor stations which receive the data from the primary GNSS satellites and a Processing Facility Centre which computes integrity and corrections forming the SBAS signal-in-space (SIS).

[56]Fisheries and Oceans Canada Coast Guard, p 11.

[57]Luís Monteiro, *Designing, configuring and validating the Portuguese DGPS Network*, PhD Thesis through Nottingham University, Nottingham, 2004.

[58]Federal Aviation Administration, *Satellite Navigation – GBAS – How it works,* https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/laas/howitworks/, (accessed on March 2017).

[59]Federal Aviation Administration, *Satellite Navigation – GBAS – How it works.*

[60]*Ibidem.*

[61]*Ibidem.*

The SBAS Geostationary (GEO) satellites relay the Signal-in-space (SIS) to the SBAS users which determine their position and time information."[62]

The U.S. established its own SBAS: Wide Area Augmentation System (WAAS), which provides real time and continental-scale augmentation. It was originally developed and activated in 2003[63] because the civilian GPS signal did not meet the aviation requirements, needing availability and better accuracy. This augmentation system operates in North America but its coverage area lasts well into South America, the Atlantic and the Pacific Oceans. There is still a separate SBAS, developed also by the U.S. only for Military use and for encrypted P(Y) code receivers called the Wide Area GPS Enhancement (WAGE).

There are other solutions apart from DGPS and SBAS that can increase GNSS' performance, such as Real Time Kinematics (RTK) and Wide Area RTK (WARTK).

The Real Time Kinematics (RTK) is used when accuracy is needed by enhancing GNSS' information precision. Basically, the system reduces and removes errors from a base and a rover station (station that collects data at remote locations[64]). Just like in any other GNSS, the position is known by calculating ranges. "At a very basic conceptual level, the range is calculated by determining the number of carrier cycles between the satellite and the rover station, then multiplying this number by the carrier wavelength."[65] These ranges still include errors that are eliminated by a system requirement including measurement transmissions from the base station to the rover station.

The Wide Area RTK (WARTK) was developed in the 90's and allows the transmission of RTK services to a greater scale (greater than 100 kilometres between the

---

[62]European Space Agency Navipedia, *SBAS Fundamentals*, http://www.navipedia.net/index.php/SBAS_Fundamentals, (accessed January 2017).

[63]GPS GOV, *Wide Area Augmentation System (WAAS) Status and History,* 2014, http://www.gps.gov/multimedia/presentations/2014/09/ION/bunce.pdf (accessed December 2016).

[64]Althos, *GPS ROVER STATION*, http://www.wirelessdictionary.com/wireless_dictionary_GPS_Rover_

Station_Definition.html, (accessed January 2017).

[65]Novatel, *Real-Time Kinematic*, http://www.novatel.com/an-introduction-to-gnss/chapter-5-resolving-errors/real-time-kinematic-rtk/, (accessed January 2017).

base and the rover stations). "The Wide-Area Real-Time Kinematics (WARTK) technique for dual and 3-frequency systems are based on an optimal combination of accurate ionospheric and geodetic models in a permanent reference stations network."[66] The only reasons for the range of the WARTK being limited to few tens of kilometres, are the differential ionospheric corrections made between the rover station and the closest GNSS station. "The ionosphere produces ambiguity biases and correlations (…). Even with the aid of multi-reference-station techniques (…) several thousand would be required to cover such a service to the whole European region."[67]

Russia began developing their space-based GNSS, "Globalnaya Navigatsionnaya Sputnikovaya Sistema" (GLONASS) in 1976[68]. Two major differences from GPS are that GLONASS has its own atomic timing reference system and does not use the WGS84 datum like GPS, using their own PZ-90 global reference system. Russia is developing – having achieved partial operational status in 2011 – its own System for Differential Corrections and Monitoring (SDCM) linked with GLONASS. The SDCM is different from other augmentation systems, as it will administer integrity monitoring for both GLONASS and GPS.

Europe decided to create its own GPS augmentation system known as the European Geostationary Navigation Overlay Service (EGNOS), coming up, later on, with the GALILEO project. Galileo was originally planned to be interoperable with GPS and Russian GLONASS and will, when concluded, consist of 30 (24 satellites plus 6 spares)[69]Medium Earth Orbit (MEO) satellites, each possessing two Rubidium Atomic

[66]European Space Agency Navipedia, *Wide Area RTK (WARTK)*, http://www.navipedia.net/index.php/Wide_Area_RTK_ (WARTK), (accessed January 2017).

[67]European Space Agency Navipedia, *Wide Area RTK (WARTK)*.

[68]Scott Madry, p 45.

[69]Vincent Reillon, p 6.

Frequency Standard (RAFS) clocks and two Passive Hydrogen Maser (PHS) clocks[70]. Galileo's first in-orbit satellites (validation elements) were launched in 2005 and 2008[71]. On December 2016, it was inaugurated with 15 operational satellites out of 18 in orbit, with an expected launch of more four satellites in November 2017.[72] Full operational capability is not expected before 2020[73].

GALILEO consists of an Open-Service (OS) with an availability of 99% and a Public Regulated Service (PRS) with an availability of 99.5%.[74]

China, on the other hand, started developing its own GNSS, having three operational satellites since the year 2000. A second generation of this system was then developed and named Compass. Nowadays, China has a modernised version of Compass – BeiDou II, which achieved operational capability since 2011. In 2015, this system consisted of 14 satellites[75], and was planned to be completely operable by 2020 (lately hastened to 2017).

India developed a Regional Satellite System. The Indian Regional Navigation Satellite System (IRNSS) consists of seven satellites with rubidium atomic clocks, in the space segment. It is also part of India's plans to create its own timing reference system and SBAS: the GPS-Aided GEO Augmented Navigation System (GAGAN). This project was developed by the Indian Space Research Organisation (ISRO), being operational for the first time in 2008[76].

---

[70]European Space Agency, *GALILEO clock anomalies under investigation*, 2017, http://www.esa.int/Our_Activities/Navigation/Galileo_clock_anomalies_under_investigation, (accessed May 2017).

[71]Vincent Reillon, p 4.

[72]*Ibidem*, p 8.

[73]*Ibidem*, p 8.

[74]European Space Agency Navipedia, GALILEO Performances, 2011, http://www.navipedia.net/index.php/Galileo_Performances, (accessed June 2017).

[75]Scott Madry, p 49.

[76]*Ibidem*, pp 51-52.

Japan, being the country with most GPS use for car navigation and other services[77], is not trying to develop its own GNSS, but has in the last decade made, just like other countries, some efforts in order to solve problems related to the use of GPS in urban canyon areas like the city of Tokyo. GPS signals can, sometimes, be reflected by tall buildings in urban landscapes (creating multi-path interference) and, as they propagate, positioning errors are generated. The Quasi-Zenith Satellite System (QZSS) started in 2002 and consists of three satellites, having its first launch in 2010 and was completed by 2013. Its design makes it totally operable and redundant when operating with other GNSS. Japan also has its own SBAS: the Japanese Multi-functional Satellite Augmentation System (MSAS), developed in 2007 and consisting of two GEO satellites in order to work with GPS and follow-on systems. [78]

As conclusion place a summary of present GNSS signals in use. Look at the graphics presented in: http://www.navipedia.net/index.php/GNSS_signal

1.2.2 What are PNT Systems?

The National Air and Space Museum Smithsonian Institution defines Position as "determining your location", Navigation as "finding your way from one place to another" and Timing as "supplying highly accurate time to synchronise complex systems".[79]

The PNT services are used by both civilian and military systems and were initially created for military-use purposes. The development of the first PNT system – GPS – started in the Sputnik era, after the first artificial satellite launched in 1957 by the Soviet Union[80]. A few years later, in the 60s, the first satellite navigation experiments were conducted by the United States' (U.S.) Navy, with the intent to track submarines carrying

[77] *Ibidem* p 52.

[78] *Ibidem*, pp 52-55.

[79] National Air and Space Museum Smithsonian Institute, *PNT (Positioning, Navigation and Timing)*, 2012, https://timeandnavigation.si.edu/multimedia-asset/pnt-positioning-navigation-and-timing, (accessed March 2017).

[80] Scott Madry, p 4.

nuclear missiles. Between 1969 and 1970[81], Ivan Getting, president of the U.S.' Aerospace Corporation, recommended the creation of a commission to analyse the progress on satellite navigation since it was an area that could be worked on and invested in.

Nowadays, there are several systems that share similar a similar complex satellite configuration and architecture with GPS. Nevertheless, PNT systems concern much more than just GNSS. These systems should provide rigorous positioning and timing information and are part of the Global Positioning System-of-Systems (GPSS)[82]. The GPSS embraces all elements - such as services, systems, components and applications[83] that are useful to worldwide users for constant PNT information update. The purpose of the GPSS is to make sure that individual systems are compatible and, even though they can be operated individually, complement each other in a more robust system.

In the last decade intense research and progress has been made in this area, with the emergence of new innovative, intelligent and robust PNT systems that accommodate various sensors and information sources.

1.2.3 Alternative PNT information sources

In 2004, the United States of America (USA) published a directive expressing the need to develop a GPS backup expressing that the "continuing growth of services based on the Global Positioning System presents opportunities, risks, and threats to the U.S. national, homeland, and economic security"[84]. The USA also stated that effort should be put into developing, deploying and operating new national security and public services or

[81]Steven Dick, Roger Launius, *Social Impact of Spaceflight*, NASA History Division, Washington DC, 2007, p 177.

[82]Jules McNeff, "Changing the Game Changer", "The Way Ahead for Military PNT", *Inside GNSS*, November/December Issue, 2010, pp 47-48.

[83]*Ibidem.*

[84]National Security Presidential Directives, *NSPD-39: U.S. Space-Based Position, Navigation, and Timing Policy*, 2004.

upgrading the existent ones; and defining the requirements and their division between the GPS and its augmentation systems.[85]

"More than 98% of the missiles currently in the U.S. arsenal have missions (…) critically dependent on GPS for achieving the required level of delivery accuracy."[86] This means that there is a need of cutting the GPS dependency, as it is vulnerable to jamming, spoofing.

Sherman Lo, senior research engineer in the GPS Laboratory at Stanford University, believes that the qualities that are mostly need in an Alternative Positioning, Navigation and Timing (APNT) system are "robustness, integrity/authenticity, and accuracy (timing and positioning)".[87] There is not, however, a consensus about how an APNT system should be and what features it should have.

The General Lighthouse Authorities of the United Kingdom and Ireland (GLA) have been pioneers in the maritime APNT research[88], especially with the development of enhanced-Loran. The Federal Aviation Administration has also developed their Distance Measuring Equipment (DME) that is a "combination of ground and airborne equipment which gives a continuous slant range distance-from-station readout by measuring time-lapse of a signal transmitted by the aircraft to the station and responded back"[89]. The Department of Homeland Security itself is looking into enhanced-Loran and Defence Advanced Research Projects Agency (DARPA) is developing chip-scale inertials.[90]

---

[85]National Security Presidential Directives

[86]Andrei Shkel, *Expert Advice: The Chip-scale Combinatorial Atomic Navigator*, http://gpsworld.com/expert-advice-the-chip-scale-combinatorial-atomic-navigator/, (accessed December 2016).

[87]Sherman Lo, "Alternative PNT: Assured Service, GNSS Backup", *Inside GNSS*, September/October Issue, 2015, pp 32-33.

[88]*Ibidem*.

[89]Skybrary, *Distance Measuring Equipment (DME)*, http://www.skybrary.aero/index.php/Distance_Measuring_Equipment_(DME), (accessed March 2017).

[90]Sherman Lo, pp 32-33.

Sherman Lo, also affirms that the solution does not go through developing or acquiring several systems due to the cost but "fewer solutions will allow us to focus on the security of each solution rather than just counting on security through diversity".[91]

The LORAN-C system used to work for the forty-eight U.S.' continental states, coastal areas and some parts of Alaska until the year of 2010[92], when the signal was terminated[93]. This system used to deliver radionavigation service for U.S. coastal waters and provided position, navigation and timing services for both civil and military air, land and marine users.

E-LORAN itself was developed from LORAN-C as feedback from the 2001 Volpe Report[94] on GPS Vulnerability. This report concentrated on the fact that the United States, just like other countries, were starting to depend only on GPS and declared it as vulnerable to intentional or unintentional interference.[95]

The main difference between eLORAN and the LORAN-C is the innovative introduction of a new data channel on the signal that is transmitted, allowing enhanced corrections, more accurate information transmitted to the receiver and optional warnings. This difference is responsible for its possible use on aircraft landing and marine navigation on harbour approaches, especially with low-visibility conditions.

Originally, e-LORAN was created by Ursanav as a navigation service using the previous LORAN-C transmitter stations at a high power level with a 100kHz frequency, but now offering bigger "accuracy, integrity, availability and continuity"[96] than LORAN-C ever offered. A particular aspect of these 100 kHz low-frequency transmissions is that they can

[91]Sherman Lo, pp 32-33.

[92]United States Coast Guard Navigation Center, *Loran-C General Information,* http://www.navcen.uscg.gov/?pageName=loranMain, (accessed October 2016).

[93]Office of Management and Budget, *Budget of the U.S. Government: Fiscal Year 2010*, U.S.A, 2010, p 40.

[94]John A. Volpe National Transportation Systems, *Vulnerability Assessment of the Transportation Infrastructure relying on the Global Positioning System, Final Report*, Massachusetts, 2001.

[95]International Loran Organisation, *Enhanced Loran (e-Loran), Definition Documen*t, 2007, p 7.

[96]Charles Curry, *Delivering a National Timescale using eLORAN*, Chronos Technology, Lydbrook, 2014, p 5.

actually penetrate through buildings in order to be used indoors (one of GPSIII's ambitions), only by using a particular object – H-field antenna (magnetic antenna).

Chronos Technology, GLA, the United Kingdom's National Physical Laboratory and Ursanav have been partners since 2011 in the e-LORAN development research project.[97] Throughout these years, several aspects have been looked at. One of them is the propagation speed of the e-LORAN signals. The speed is higher over seawater[98] so it is easier to know the time delay due to the actual propagation through the atmosphere – this delay is known with great precision. Nevertheless, the propagation over land is slightly slower because there is a bigger signal delay, known as the Additional Secondary Factor (ASF). The ASF can reach a significance of several microseconds. All the existing e-LORAN stations have their ASF predicted by using a computing model, due to the different values of the earth's conductivity that lead to the signal's attenuation (and varies in different planet regions). This ASF value is measured instantly when the timing receiver is firstly operated, which means that it can vary with the seasons or atmospheric conditions. For that reason, the eLORAN Differential Time Receiver (EDTR) was used, so that corrections can be made and sent to the receiver by the new operational LORAN Data Channel (LDC).

Figure 2 shows the difference of three different parameters (Accuracy, Integrity and Availability) between LORAN-C and eLORAN.

Performance	USCG Loran-C	Modernised Loran-C	Prototype eLoran	eLoran
Accuracy (95%)	460m	100m	10-20m	10-20m
Integrity	Low	Moderate	High	High
Availability	Low	Moderate	Moderate	High

Figure 2 - Generations of Loran's performance[99]

[97]Charles Curry, *Delivering a National Timescale using eLORAN*, p 5.

[98]*Ibidem*, p 7.

[99]General Lighthouse Authorities of the United Kingdom and Ireland, "Briefing note: Evolution from Loran-C to eLoran", p 3.

When eLORAN is used for positioning, at least three stations are needed (calculating a two-dimensional position fix and time). Nevertheless, additional stations offer bigger information accuracy.

Differential eLORAN, consists of an eLORAN receiver equipped with an external H-field antenna. It was developed with the intention of improving the positioning's accuracy with ASF corrections. In order to have full Differential eLORAN service for harbour approach and entrance, there must be at least three eLORAN transmitters close to the harbour as well as a Differential eLORAN Reference Station that can make the respective variable ASF correction that can occur due to seasonal, daily or weather variations.

Some countries are making an effort to implement eLORAN technologies or to upgrade their obsolete LORAN-C equipment. South Korea is one of the countries investing in the eLORAN system due to the GPS jamming incidents that it has been suffering in the past few years. Figure 4 shows a table of actually known and confirmed incidents that they suffered.

Dates	August 23-26, 2010 (4 Days)	March 4-14, 2011 (11 Days)	April 28 – May 13, 2012 (16 Days)
Jammer Locations	Kaesong	Kaesong, Mount Kumgang	Kaesong
Affected Areas	Gimpo, Paju, etc.	Gimpo, Paju, Gangwon	Gimpo, Paju
GPS Disruptions	181 cell towers 15 airplanes 1 battleship	145 cell towers 106 airplanes 10 ships	1,016 airplanes 254 ships

Figure 3 - Korean jamming incidents[100]

South Korea's eLORAN initial implementation plan consisted in upgrading their old LORAN-C stations to eLORAN; building three new eLORAN stations; and having forty-three

[100]General Lighthouse Authorities of the United Kingdom and Ireland, "Briefing note: Evolution from Loran-C to eLoran", p 3.

differential eLORAN stations that would cover the whole country with 20m accuracy[101]. This initial plan was improved to a new "Revised Korean e-LORAN Plan"[102] that consists in two-phase access: the first phase consisted in implementing maritime e-LORAN for the west sea of Korea by the end of the year 2015 (which still is not completed and should only be so by the end of 2019[103]) and if it turns out to be useful and reliable, expand it by implementing more transmitters and differential stations (second phase).[104]

In 2014 there were nine Northern European available eLORAN stations (one in the United Kingdom (Anthorn), Germany (Sylt) and Denmark (Faroe Islands)), two in France (Lessay and Soustons) and four in Norway (Vaerlandet, Boe, Jan Mayen and Berlevag), all used in Prototype e-LORAN mode)[105]. The Netherlands declared their first differential eLORAN implementation in the Port of Rotterdam, in December 2015, which uses signals from France, Germany and the United Kingdom[106].

In the end of 2016, France lost interest and shut down its stations. Norway also lost interest stating that it is "outdated and has very few users"[107]and Denmark will lose the French financial support on its Faroe Island transmitter[108]. This means that if these eLORAN sites are completely erased, it will be hard to continue an implementation plan

[101]Federal Aviation Administration, *The Global Loran/eLoran Infrastructure Evolution, A Robust and Resilient PNT Backup for GNSS,* USA, 2014, p 31.

[102]*Ibidem*.

[103]Japan Times, "South Korea revives GPS backup project after alleged jamming by North Korea", 2016, http://www.japantimes.co.jp/news/2016/05/02/asia-pacific/south-korea-revives-gps-backup-project-after-alleged-jamming-by-north-korea/#.WAVG1eArLIV, (accessed October 2016).

[104]Federal Aviation Administration, *The Global Loran/eLoran Infrastructure Evolution*, p 32.

[105]*Ibidem*, p 20.

[106]Dee Ann Divis, "Proposal for U.S. eLoran Service Gains Ground", 2014, http://www.insidegnss.com/node/3853, (accessed October 2016).

[107] Royal Institute of Navigation, "UK eLoran abandoned", 2016, https://www.rin.org.uk/NewsItem/4433/UK-eLoran-abandoned, (accessed May 2017).

[108] Charles Curry, *GPS-Free UTC TimeScale Using eLoran*, International Timing and Sync Forum 2015, Edinburgh, 2015, p 15.

and the United Kingdom's station will only be able to provide timing – limited in a way – as positioning will not be possible without trilateration.[109]

The U.S., on the other hand, are still in the process of dismantling its old LORAN-C stations instead of investing in upgrading them to e-LORAN, for GNSS redundancy. As said by the Office of Management and Budget, on 2010's financial year budget, "the Nation no longer needs this system because the federally-supported civilian Global Positioning System has replaced it with superior capabilities"[110].

It is hard for the United States to take a position or make any statement when Europe is falling back from this project. As said by Professor David Last, "the question is whether we are going to have an Eastern Europe with a clear fall-back to an eLORAN-type (*e-Chayka*) system, and Western Europe switching theirs off".[111] He also pointed out that what Europe actually needs is to see that the U.S. are also interested in eLORAN: "the U.S. are very influential, and if the U.S. are going to stand up and say, 'We're bringing eLORAN back' — that in itself would be a very powerful message"[112].

One of the countries that deserves emphasis is the United Kingdom due to the great effort that Chronos Techonology has been putting in the eLORAN implementation plan. Chronos has been responsible for the GNSS Availability Accuracy Reliability and Integrity Assessment for timing and Navigation (GAARDIAN Project) and the GNSS Services Needing Trust in Navigation, Electronics, Location & Timing (SENTINEL Project). The United Kingdom has its eLORAN system operating with GPS since May 2010.[113] In 2010, Chronos and GLA analysed the existing options in order to provide resilient PNT and to

[109]David Last, "U.S. Nears eLoran Decision with Broad International Implications", *Washington View – Inside GNSS*, March/April Issue, 2015, pp 24-31.

[110]Office of Management and Budgets*, Terminations, Reductions, and Savings, Budget of the U.S. Government,* Washington D.C., 2009.

[111]David Last, pp 24-31.

[112]*Ibidem.*

[113]Paul Williams, David Last, Nick Ward*, The Deployment of eLoran in the UK*, General Lighthouse Authorities of the United Kingdom and Ireland, Harwich, 2013, p 1.

follow IMO's advice on the adoption of an e-Navigation strategy.[114] The research developed by GLA led to the conclusion that the implementation of eLORAN would allow the reduction of the Aids-to-Navigation (AtoN) infrastructure and the removal of some lights and physical aids. This would reduce the yearly overall costs.

Another alternative PNT information source is Inertial Navigation. "Inertial Navigation is a self-contained navigation technique in which measurements provided by accelerometers and gyroscopes are used to track the position and orientation of an object relative to a known starting point, orientation and velocity".[115] It is also a basic form of navigation and consists on knowing your initial position, velocity and orientation and then measuring your orientation changes and acceleration, without relying on external references. Inertial sensors themselves, measure the rotation rate and acceleration using gyroscopes and accelerometers, respectively. Normally, three orthogonal rate-gyroscopes and three orthogonal accelerometers make an Inertial Measurement Unit (IMU).[116]

An Inertial Navigation System normally consists of an IMU, Instrument Support Electronics and Navigation Computers to integrate and maintain the position estimate.[117] The IMU itself can have two types of configurations: Strapdown Systems or Stable Platform Systems. The Strapdown Systems as the actual name says, have their sensors rigidly attached to the device. This reduces the cost and, also, the mechanical complexity. The Stable Platform Systems have the inertial sensors mechanically isolated from rotational motion and installed in a stable platform. This method is widely used when high accuracy is needed, mostly in ships and submarines. These systems can also be called Gimbaled Inertial Platforms and normally three of them are needed to protect a system from three axes rotations: roll, pitch and yaw.

---

[114] International Maritime Organisation, Subcommittee on the Safety of Navigation, *Report to the Maritime Safety Committee*, IMO, 2011, p 18.

[115] Oliver Woodman, *An Introduction to Inertial Navigation*, 2007, p 5.

[116] Tampere University of Technology, *Basic Principles of Inertial Navigation*, http://aerostudents.com/files/avionics/InertialNavigationSystems.pdf, (accessed December 2016).

[117] *Ibidem*

The advantages of Inertial Navigation Systems are that they do not need external references (only an initial position) and are autonomous; they are immune to jamming and spoofing and do not need any antenna that can be radar detected (important in a warfare scenario), unlike other PNT Systems. On the other hand, the error increases with time (as the only real position is the first one); high acquisition and maintenance costs compared to GPS; and higher power requirements than GPS.[118]

In the beginning of 2017, DARPA started developing a vibration and shock-tolerant inertial sensor that, they believe, will mitigate the need of GPS. This project, named ATLAS, "will deliver a comprehensive approach to breaking performance and cost, size, weight and power barriers in inertial sensor technology that prevent robust, GPS-independent, military positioning, navigation and guidance"[119]. The project consists in making a combination of a micro-electro-mechanical systems with a Coriolis Vibratory Gyroscope which can be seen in Figure 4 below.

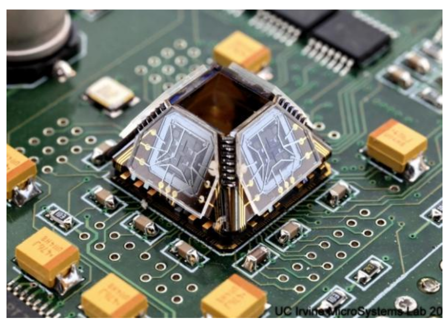


Figure 4 - Micro-electro-mechanical System Coriolis Vibratory Gyroscope[120]

Nevertheless, there is a big engineering challenge within that consists in creating a whole new system architecture that can transfer the stability from the atomic time reference to the Coriolis Vibratory Gyroscope without increasing the Signal-to-Noise Ratio (SNR).

[118]Tampere University of Technology.

[119]GPS WORLD, "HRL Labs to develop inertial sensor tech for DARPA", *GPS WORLD*, 2017, http://gpsworld.com/hrl-labs-to-develop-inertial-sensor-tech-for-darpa/, (accessed January 2017).

[120]Paul Buckley, "Next-gen inertial sensors aim to replace GPS", *Smart2zero*, 2016, http://www.smart2zero.com/news/next-gen-inertial-sensors-aim-replace-gps, (accessed July 2017).

DARPA is focusing on reducing the GPS reliance by providing redundant capabilities and designing new PNT solutions. Some of their main goals include creating ultra-stable clocks and providing PNT systems in new environments such as indoor, underwater and underground, where GPS is not capable of providing fixing solutions. To achieve these goals, DARPA started a project in 2012 named Chip-Scale Combinatorial Atomic Navigator (C-SCAN).[121] The final product of this project should be a small IMU that brings atomic and inertial sensors together in a microsystem, with a very high motion detection, combining both gyroscopes and accelerometers, designed in order to provide more accurate and precise inertial navigation, in a very small and scrupulous way.

Pseudolites are, also another PNT alternative, according to the Federal Aviation Administration APNT Research Program[122]. Having its use been recommended since late 70's and early 80's[123], the term Pseudolites comes from the merging of the two terms "Pseudo" and "Satellites". A very important demonstration took place in the White Sands Missile Range (a military testing area in New Mexico) in 2011[124] with the support of DARPA. Although Pseudolites are satellite-like transmitters (with a transmitter and a receiver just like GNSS), they have their signals transmitted much closer to earth than GPS satellites. To determine the location, the transmitter, which has an anti-jam antenna, sends a signal to a modified GPS receiver which makes a range measurement.

Pseudolites use several geographical separate terrestrial transmitters to offer passive pseudo ranging signals.[125] There are several intrinsic benefits like unlimited user capacity and, also, the possibility of transmitting signals from different equipment, like a Distance Measuring Equipment (DME) or a Ground Based Transceiver (GBT), reducing the number of terrestrial stations needed. The total travel time of the signal can be calculated

---

[121]Andrei Shkel, "The Chip-scale Combinatorial Atomic Navigator", GPS WORLD, August Issue, 2013, pp 8-10.

[122]Sherman Lo, *Pseudolite Alternatives for Alternate Positioning, Navigation and Timing (APNT)*, p 1.

[123]Cillian O'Driscoll, Daniele Borio, Joaquim Fortuny, *Scoping Study on Pseudolites*, European Commission Joint Research Center, 2011, p 1.

[124]Kathryn Bailey, *Moving Celestial To Terrestrial: Leveraging Pseudolites For Assured PNT*, http://www.cerdec.army.mil/news_and_media/Moving_celestial_to_terrestrial_leveraging_pseudolites_for_Assured_PNT/, (accessed December 2016).

[125]Cillian O'Driscoll, Daniele Borio, Joaquim Fortuny, p 1.

using the signal's Time of Arrival (TOA), more specifically, from the time difference between transmit time indicated by the ground clock and received time measured by the user clock. Nevertheless, the clock synchronization to the ground clock must be known. Three stations are needed for passive ranging but, as said above, the use of DME and GBT may reduce station need.

The Satellite Time and Location (STL) Service, developed by Iridium Communications Inc., consists of 66 cross-linked, low-earth orbit satellites.[126] This technology can be included in several types of devices, as it is chip-size, and can make it much harder to spoof or jam GPS receivers operating this system. STL also has a unique code for each ground position which makes the system only usable if the user is in the right and expected position. Some of the advantages of this service are that it is already in space, tested and ready to use; its low earth orbit satellites allow a significate stronger signal than GPS (which is much harder to jam); it is independent to any other technology and it will also be supported by Iridium NEXT (next-generation global satellite generation) supposed to be concluded at the end of 2017.[127]

The Network Time Protocol (NTP) was developed by Professor David L. Mills, at the University of Delaware in 1985.[128]Since then, NTP has been used as an online protocol for time synchronization on computers and Local Area Networks and, also, an alternative for time reference. Atomic clocks are the most reliable timing devices, but can be very expensive. NTP synchronizes, using UTC as reference time[129], to a reliable timing source: it could be an actual computer, a watch or even an atomic clock in a GPS satellite.[130] This system selects the best available time source, which means, more sources lead to smaller

---

[126]GPS WORLD, "Iridium launches alternative GPS PNT service", *GPS WORLD*, 2016, http://gpsworld.com/iridium-launches-alternative-gps-pnt-service/, (accessed January 2017).

[127]GPS WORLD, "Iridium launches alternative GPS PNT service".

[128]Richard Williams, *What is NTP*, http://www.galsys.co.uk/time-reference/basic-ntp/what-is-ntp.html, (accessed March 2017).

[129]NTP FAQ, *What is NTP?*, http://www.ntp.org/ntpfaq/NTP-s-def.htm#AEN1259, (accessed March 2017).

[130]Richard Williams.

errors. Also, it identifies and excludes senseless time sources.[131] If the network connection is, somehow, temporarily unavailable the NTP uses past measurements to predict the actual time and possible error.[132]

The Automatic Identification System (AIS) is commonly used in marine navigation as it has the capability of transmitting diverse information like speed, course, position (obtained from a GNSS receiver)[133]. The fact that the position is obtained by a GNSS receiver aboard, makes this system GNSS dependent. "The Automatic Identification System Autonomous Positioning System (AAPS) is comprised of a master AIS base station, some slave base stations, a shipborne AIS equipment and an ASF correction system."[134] The time synchronization of the system is assured by the intercalary transmission of the base station and the slave base stations, which signals are received by the AIS equipment aboard and, posteriorly, an ASF correction system leads to better positioning accuracy by reducing propagation errors. [135]. It is possible to have autonomous positioning on the AIS by measuring VHF radio signals from the actual base stations to the AIS equipment. "In the AAPS, the AIS base stations are time synchronized. The shipborne AIS can measure the transmission delay of the VHF AIS signal from the AIS base stations." Then, it is possible to know a vessel's true position (calculated through the signal's travelling time).[136]

Multisensor navigation is, also, a resilient alternative for PNT information as GNSS, alone, cannot respond to various factors that have been referred throughout this study[137].

---

[131]NTP FAQ.

[132]*Ibidem.*

[133]Qing Hu, *Development of an Automatic Identification System Autonomous Positioning System*, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4701297/, (accessed March 2017).

[134]*Ibidem.*

[135]Qing Hu.

[136]*Ibidem.*

[137]Grejner-Brzezinska, *et al*., "Multisensor Navigation Systems: A Remedy for GNSS Vulnerabilities?", *Proceedings of the Institute of Electric and Electronics Engineers*, Vol. 104 nº 6, June 2016, p 1342.

Although a big effort has been made in the last decade to create new resilient PNT alternatives, little effort has been made to bring them together.[138]

Multisensor navigation can be obtained by coupling several sensors together in order to build a resilient, available and robust system. An example of several sensors that already exist and could be brought together in a car navigation system, can be seen on Figure 5 below.

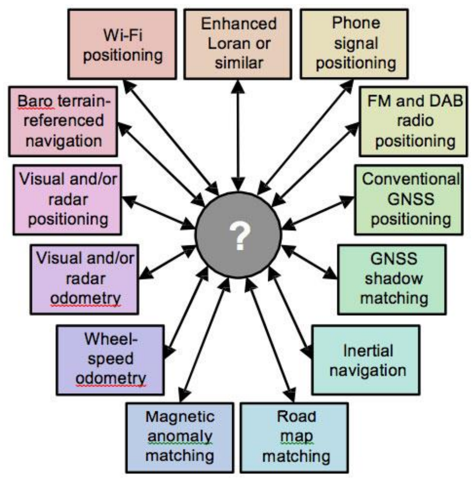


Figure 5 - Multisensor navigation for a car navigation system[139]

There are two basic solutions to complement GNSS' information: supervising the received GNSS signal and/or adding other sensors' data. This can be possible through a Receiver Autonomous Integrity Monitoring (RAIM) technology that, other than integrating all the positioning solutions, also can acquire and recognize system failures. Nevertheless, RAIM is signal dependent for positioning determination, which means it is not a PNT solution. [140]

The systems presented above are some of the PNT alternatives that are already being used in several countries or still in development and implementation. A general knowledge about these systems should be known in order to adopt a resilient PNT strategy through redundancy or upgrading the already existent systems.

---

[138]Alan Cameron, "A long look at advanced Multisensor Navigation and Positioning", *GPS WORLD*, 2014, http://gpsworld.com/a-long-look-at-advanced-multisensor-navigation-and-positioning/, (accessed July 2017).

[139]*Ibidem.*

[140]Grejner-Brzezinska*, et al.*, p 1343.

1.2.4 How to seek resilience in a PNT System?

The GNSS when used for positioning, navigation and timing can have serious flaws due to the distance of the actual satellites to the receivers. The signal's power is very low and vulnerable to interference, ionospheric effects, jamming and spoofing[141]. Jamming and Spoofing cannot be anymore declared as rare events as it is becoming easier and easier, every day, to acquire jamming and spoofing equipment online. The year of 2017 was marked by the release of the Pokémon Go game. Common players were jailbreaking their phones and managing to fake GPS positions so they could complete the game without having do wander through the streets. This is spoofing and it is possible to be achieved in just about 90 seconds.[142]

Atmospheric effects are also very important to consider. "Space weather disturbs the ionosphere to an extent where the model no longer works and large pseudo range errors, which can affect position and timing, are generated".[143]

Apart from the flaws that were referred, GNSS also has segment errors that can also generate user problems. In 2014, incorrect ephemeris data was uploaded in the Russian GLONASS satellites, causing positioning, navigation and timing information issues for about half a day.[144]

When developing or implementing a new PNT system, the main objective should be to "ensure the highest levels of data integrity"[145] and for that reason "the underlying

---

[141]The Royal Academy of Engineering, *Global Navigation Space Systems: reliance and vulnerabilities*, London, 2011, p 8.

[142]Gohub, "In 2017, GPS Spoofing is the real bane of Pokémon GO, 2017", https://pokemongohub.net/2017-gps-spoofing-real-bane-pokemon-go/, (accessed May 2017).

[143]GPS WORLD, "Make it real: Developing a test framework for PNT systems and devices", http://gpsworld.com/make-it-real-developing-a-test-framework-for-pnt-systems-and-devices/, (accessed January 2017).

[144]*Ibidem.*

[145]McMurdo, *Resilient PNT, At the Core of Mission Critical Applications*, http://www.mcmurdogroup.com/company/orolia-group/what-is-resilient-pnt/, (accessed May 2017).

PNT technologies, products and systems must be resilient.” For that reason, according to the International Maritime Organisation (IMO), a resilient PNT system should have the following functionalities or characteristics[146]:

- Serve general navigation (including harbour entrances and approaches);
- Be compatible with local augmentation (if this item is not already provided);
- Unlimited number of users;
- Low user cost;
- Should operate with geodetic and time reference systems;
- Provide the user with position, time, course and speed over ground information;
- Inform the users when system degradation occurs;
- Be compatible with other shipborne equipment (Electronic Chart Display Information System (ECDIS), Automatic Identification System (AIS), GMDSS to offer them vessel data;
- Accuracy - “The degree of conformance between the estimated or measured parameter of a craft at a given time and its true parameter at that time.”[147]
- Availability - “The percentage of time that an aid, or system of aids, is performing a required function under stated conditions.”[148]
- Continuity– “The probability that, assuming a fault-free receiver, a user will be able to determine position with specified accuracy and is able to monitor the integrity of the determined position over the (short) time interval applicable for a particular operation within a limited part of the coverage area.”[149]

---

[146] International Maritime Organisation, *Resolution A.915(22), Revised Maritime Policy for a Future Global Navigation Satellite System*, 2011, pp 68-79.

[147] International Maritime Organisation, *Resolution A.915(22), Revised Maritime Policy for a Future Global Navigation Satellite System,* p 71.

[148] *Ibidem*, p 71.

[149] *Ibidem*, p 71.

- Integrity monitoring – "The process of determining whether the system performance (or individual observations) allow use for navigation purposes."[150]
- Integrity risk – "Integrity risk. The probability that a user will experience a position error larger than the threshold value without an alarm being raised within the specified time to alarm at any instant of time at any location in the coverage area."[151]
- Redundancy – "The existence of multiple equipment or means for accomplishing a given function in order to increase the reliability of the total system."[152]
- Reliability on its observations – "A measure of the effectiveness with which gross errors may be detected. This internal reliability is usually expressed in terms of marginally detectable bias."[153]

Another way of seeking the resilience of a PNT System is by improving the existent ones. The United States' Department of Homeland Security did a report on the improvement of the operation and development of GPS. Throughout this report they referred several means to improve the resilience of equipment receiving GNSS signals[154], such as:

- Employing Obscure antennas[155] – not visible from public access areas or physically hiding the antennas (ex: plastic fencing);

[150]International Maritime Organisation, *Resolution A.915(22)*, p 73.

[151]International Maritime Organisation, *Resolution A.915(22), Revised Maritime Policy for a Future Global Navigation Satellite System,* p 71.

[152]*Ibidem*, p 74.

[153]*Ibidem*, pp 74.

[154]United States Department of Homeland Security, *Improving the Operation and Development of the GPS Equipment Used by Critical Infrastructure*, United States Department of Homeland Security, 2017, pp 5-7.

[155]*Ibidem*, p 5.

- Employing Decoy antennas[156] – using clear visible antennas in a public access area far from the actual antenna;
- Wisely selecting antenna locations[157] – installing the antenna from and above (at least 10 meters) close structures for a great multipath environment with an unobstructed sky-view;
- Blocking antennas[158] – protecting the receiver from interference, jamming and spoofing;
- Implementing redundancy[159] – have two or three antennas in different locations with different receivers for outputs comparison;
- Calibrating[160] – evaluating the delay variations;
- Steering clear from low elevation signals[161] – they are attenuated from horizon-nulling antennas (below 25º degrees elevation);
- Using position hold for stationary timing receivers[162] – timing receivers that operate in position hold, needing only information from one satellite for timing information;
- Using high-quality devices[163] - timing receivers should have an atomic clock as backup. Positioning can be backed up by inertial systems;
- Adding a sensor/blocker[164] – sensors that detect jamming, spoofing or interference and report to monitoring sites, also collecting this data for

[156]United States Department of Homeland Security, p 5.

[157]*Ibidem*, p 5.

[158]*Ibidem*, p 5.

[159]*Ibidem*, pp 5-6.

[160]*Ibidem*, p 6.

[161]*Ibidem*, p 6.

[162]*Ibidem*, p 6.

[163] *Ibidem*, p 6.

[164] *Ibidem*, p 6.

investigation. The blocker can also block radiofrequency inputs when one of these events is detected;

- Practicing cyber hygiene[165] - GNSS receivers and data processors are computers that should have firewalls, anti-virus software and authentication with strong passwords.

[165] United States Department of Homeland Security, pp 6-7.

Chapter 2 – GNSS Vulnerabilities

2.1 Vulnerabilities

There are several GPS sources of errors, per example:

- Errors in the ephemeris data transmission (ex: in the transmission of the satellite's location) – this error is the difference between the expected and actual position of the satellite[166];
- Satellite clock errors – although atomic clocks are accurate there isn't perfectly accurate synchronization between the timing of the satellite broadcast signals and the GPS system time[167];
- Ionospheric effects that cause pseudorange correction errors which will be referred further on in this section;
- Multipath errors caused by reflected signals on the antennas – signals don't always travel straight to the antenna as they can be reflected by obstacles, which makes antennas receive direct and reflected signals[168] ;
- Errors of the actual receiver (clock synchronisation with satellites, thermal noise and software accuracy)[169].

These sources of errors make GNSS systems vulnerable. Also, intentional or unintentional events like Interference; Scintillation; Jamming and Spoofing may occur.

In January 2016, many GPS satellites broadcasted timing errors for a period of nearly 12 hours. The United Kingdom's Space Agency and the Royal Institute of Navigation

[166]How GPS works, http://www.how-gps-works.com/glossary/ephemeris-error.shtml, (accessed July 2017).

[167]Bharati Bidikar, *et. al*., "Satellite Clock Error and Orbital Solution Error Estimation for Precise Navigation Applications", Scientific Research, 2013, p 23.

[168]Trimble, *Trimble GPS Tutorial - Error Correction*, http://www.trimble.com/gps_tutorial/howgps-error2.aspx, (accessed July 2017).

[169]Civil Engg Dictionary, *Sources of errors in GPS*, http://www.aboutcivil.org/sources-of-errors-in-gps.html, (accessed July 2017).

developed a report about this incident and concluded that the cost of GNSS disruption can reach 1 billion pounds sterling per day. The report focuses on “ten application domains in the United Kingdom (UK): Road, Rail, Aviation, Maritime, Food, Emergency and Justice Services, Surveying, Location-Based Services (LBS), Other Infrastructure, and Other Applications.”[170]

In this report, an important upshot was presented, according to the January 2016 incident: “A day in the UK without GNSS”. The most important facts, which were felt by normal user citizens, are summarized in Table 1.

[170]Alan Cameron, “Double trouble: GNSS over-reliance and its costs”.

"A day in the UK without GNSS"	
At home	Most activities are not affected (apart from the morning run and weather forecast).
On the move	Journey must me memorized/paper maps; More vehicles on the road (taking slower to consult paper maps); On trains, there is not information on the next departure; Queue on the phone line for calling cabs (app does not work).
With others	Not possible to track children; Friends no longer share their location; Augmented reality games do not work.
At the shops	Supermarket shelves run out of products; People hoard products and higher priced black market may emerge; Delivery of online shopping loses efficiency.
When things go wrong	More time handling emergency calls; First responders (police, ambulance and fire services) cannot use location to navigate to an incident; Lone works loses the safety that someone is able to support them.
Back at home	The groceries or take-away food is delayed.

Table 1 – Impact of "A day in the UK without GNSS"[171]

2.1.1 Interference

Interference occurs when unwanted signals interfere with actual GNSS signals leading to the loss of accuracy or even denying system function.[172] This occurs due to the weakness of the signals that can be up to a hundred times weaker than the background noise. Also, even though the GNSS bands are protected, there are many signals being transmitted in close frequencies and those, sometimes, cause interference.[173] Normally, some part of the background noise can be removed as well as similar signals that get

[171] Innovate UK, The UK Space Agency, The Royal Institute of Navigation, *Economic Impact of a disruption to GNSS, Showcase Report*, London, London Economics, 2017, p 6.

[172] Septentrio Satellite Navigation, *GNSS Interference*, Belgium, 2012, p 3.

[173] *Ibidem*, p 4.

spilled on the GNSS bands, but some still manage to persist. An example of possible interference is that the GLONASS L2 band shares some frequencies with radio amateur bands. This can lead to temporary losses of GNSS signals in some countries. "A source of interference is likely to affect multiple signals in the same GNSS band and may entirely block reception of a whole GNSS band."[174]

2.1.2 Ionospheric effects

GNSS signals pass through the Ionosphere until they reach the earth's surface receivers. There are free ionosphere electrons that have been separated from atmosphere atoms through the sun's ultraviolet light.[175] In the night period, as there is so sunlight, these electrons tend to reunite with the atoms. GNSS signals, on their way to the earth's surface, can be refracted by these electrons changing their travelling path and speed. Although this process is important and must be taken into account in order to maintain GNSS accuracy and availability, there is another important occurrence: scintillation. "Scintillation occurs when irregularities in the electron density of the ionosphere cause rapid changes in the phase and amplitude of the transmitted signals."[176] This factor may lead to the loss of the GNSS signals, as they will be ignored by the receivers due to the different signal characteristics.

Normally, the sun's radiation and ionization process is quite constant, which makes it possible to correct most measurements and keep high accuracy. Nevertheless, there can be sporadic sun storms that lead to an enormous increase of electrons in the ionosphere. This phenomenon, as it happens occasionally, is difficult to predict and may lead to the temporary loss of GNSS information.[177]

---

[174] Septentrio Satellite Navigation, p 5.

[175] Richard Langley., "Innovation: GNSS and the Ionosphere", *GPS WORLD*, 2011, http://gpsworld.com/innovation-gnss-and-ionosphere-11036/, (accessed May 2017).

[176] Richard Langley.

[177] *Ibidem.*

2.1.3 Jamming and jamming trials

"Jamming devices are radio frequency transmitters that intentionally block, jam, or interfere with lawful communications, such as cell phone calls, text messages, GPS systems, and Wi-Fi networks."[178]

As there is a considerable distance between the GPS' satellites and the earth's surface, they are easy to jam. A GPS jammer can send its own signals on the same frequency than the GPS bands, increasing the SNR and, consequently, preventing the GPS receiver from receiving any signals. GNSS jamming devices can be mostly divided in two categories: GPS only and GPS and mobile communications. Jammers - of both categories - can be bought for less than a hundred dollars, depending on its power, and are considered illegal to market, sell or use in the United States of America.[179]

There are several ways of protecting against jamming such as using Radio Frequency (RF) filters on the receiver (if the jamming signal overpowers the GPS signal and falls right in-band, it still might not be the best method); using IMU's as said before; using multiple antenna arrays with various directions in order to acquire signals from multiple directions (to prevent from being affected by the effective range of the jamming signals)[180]; using a Controlled Radiation Pattern Antenna (CRPA) that consists in an antenna array and processing unit that phase-destructs (nulls) any interfering signals. A CRPA consists of seven patches, each one with a low-noise amplifier and two filters for out-of-band rejection. [181]. The last and probably to most effective way, is investing in new PNT alternatives that are not vulnerable to jamming.

---

[178]GPS.GOV, *Information About GPS Jamming*, http://www.gps.gov/spectrum/jamming/, (accessed January 2017).

[179]*Ibidem.*

[180]Novatel, *Understanding the Difference Between Anti-Spoofing and Anti-Jamming*, http://www.novatel.com/tech-talk/velocity/velocity-2013/understanding-the-difference-between-anti-spoofing-and-anti-jamming/, (accessed January 2017).

[181]GPS WORLD, "Anti-jam Protection by Antenna", 2013, http://gpsworld.com/anti-jam-protection-by-antenna/, (accessed June 2017).

The SENTINEL Project Report on GNSS vulnerabilities enumerated several jamming mitigation techniques such as giving more importance to resilient timing (by using Oven Controlled Oscillators, Rubidium Clocks and Chip Scale Atomic Clocks) which preserves accurate timing in a GPS-denied environment; the use of multiple GNSS has also been a troubled option as nearly all the GNSS share the same or similar frequencies apart from the Russian GLONASS[182]; and at last, having been referred before, implementing e-LORAN, that may be up to a future shutdown.

In the Portuguese Navy, more specifically, no internal doctrine could be found, throughout this research, of which antennas should be used or how they should be positioned aboard. This means that if an assessment on this matter is made, it is possible to find out in which way they antennas be less vulnerable to interference depending on their type and where they should, originally, be installed.

Several jamming trials have been taken before and after the SENTINEL Project in three different places. The first one took place in Sennybridge (Wales), the second one in Nuneaton (England) and, the third, in Sweden.

The Sennybridge jamming trial was the first non-military trial using civilian jammers, divided by three sessions: June 2011, June and October 2012 and 2015. One of the conclusions that was extracted from these trials was that the Portable jammers' effective range was much larger than what the sellers predicted.

The Nuneaton trial took place, mainly, to test the CTL3520, a hand-held jamming detector, which was a 100% successful. The jammer was placed in a car boot. The car was quickly identified and the jammer equipment was removed. The CTL3520, developed by the University of Bath in the United Kingdom for the SENTINEL Project, is capable of searching and finding the direction of a jammer, operating on the GPS L1 band.[183]

The Swedish Trial was, also, mainly performed to test the CTL3520's direction finding capability.

[182]Charles Curry, *Sentinel Project, Report on GNSS Vulnerabilities*, Chronos Technology, Lydbrook, 2014, p 31-33.

[183]*Ibidem*, p 34.

In 2015, during the Annual Navigation Warfare trial hosted by the United Kingdom Ministry of Defence, several GPS equipment and GANDALF MkII - a jammer detector - were tested. GANDALF MkII estimates the jamming signal's Direction of Arrival. If this process is done several times, the true position of a jamming source can be identified as well as it helps the operator find out which type of jammer is being used.[184]

In April 2008, the GLA in partnership with the United Kingdom Government's Defence Science and Technology Laboratory performed a jamming trial near Flamborough Head (near the North Sea), using the vessel NLV "Pole Star".The objectives and results of this trial are described on table 2[185] below.

Objectives	Results
Test GPS denial impact on maritime safety	The vessel was able to navigate using radar and traditional navigation techniques.
How mariners cope with GPS information loss	Loss of GPS caused many alarm sounds on the bridge (chaos).
How DGPS is affected by GPS Jamming	DGPS station in Flamborough Head was affected by GPS jamming (station went "unhealthy" and as the alarms went off, locked up).
Test e-LORAN as a GNSS back-up system	e-LORAN service was not affected.
Effect of GPS Jamming on Automatic Identification System (AIS)	GPS jamming affected the AIS (lost range and bearing information) and the nearby Maritime Coastguard Agency received erroneous data.
Effect on synchronized light units and systems	If there is GPS denial when they are first turned on, they fail to synchronize. Once synchronized they use their internal clock (synchronises with GPS every 20 minutes).
Effect of GPS denial on communications systems	Digital Selective Calling (DSC) kept working through jamming periods yet failed to offer accurate positioning information. Communication systems worked continuously.

Table 2 - Table 2 - NLV "Pole Star" Jamming Trial Results

[184] North Atlantic Treaty Organization, *Testing direction finder at GPS Jamming Trials*, https://www.ncia.nato.int/NewsRoom/Pages/160905-Sennybridge-GPS-Jamming-Trials.aspx, (accessed January 2017).

[185] General Lighthouse Authorities of the United Kingdom and Ireland, *GPS Jamming Trial, Executive Summary Report for Website*, United Kingdom, 2008, p 4-5.

Several conclusions were taken by the GLA from this trial such as:

- GPS having great impact on maritime safety;
- During a jamming trial the Vessel Traffic Service (VTS), obtains erroneous vessel positioning data (such as vessels travelling over land);
- If AIS is used as an AtoN, it can broadcast incorrect information which can be completely dangerous for maritime safety;
- In ships DSC emergency communications can be lost if they are based on GPS;
- The loss of GPS information can have a very big impact on mariner's as they will have to firstly identify the problem, secondly, be familiar with more rudimental navigation techniques in order to always now the vessel's position and at last, have the ability to keep calm as alarms sounding on the bridge can be a "stress" factor.[186]

In 2009, another Jamming Trial was taken by the GLA, but this time in Newcastle-Upon-Tyne[187] and using another vessel: THV "Galatea". This time, when the jamming signal was low no alarms sounded. However, there was absurdly erroneous positioning and speed information. As the jamming signal was intensified, alarms started to sound on the bridge until the Electronic Chart Display System (ECDIS), the Autopilot, the DGPS, the DSC, the Radar, the Gyro-compass and the AIS failed completely.[188]

2.1.4 Spoofing and spoofing trials

Spoofing can be achieved through a complex signal generator that recreates signals from various GPS satellites. Firstly, knowing the actual true position, this signal is

[186]General Lighthouse Authorities of the United Kingdom and Ireland, *GPS Jamming Trial,* p 5-6.

[187]Alan Grant, Paul Williams, Sally Basker, "GPS Jamming and its impact on maritime safety", *Port Technology International*, 2010, pp 39-41.

[188]George Shaw, *et al*., *Mitigating the effects of GNSS Interference – GLA monitoring and update on eLoran*, General Lighthouse Authorities of the United Kingdom and Ireland, 2011, p 9.

transmitted to a GPS receiver[189] . When the receiver accepts this signal it is possible to simulate positions. These signals should be strong enough to prevail against true GPS signals but not too strong to be ignored and originate system failure. This makes it harder to discover when a spoofing attack occurs as there is no system failure and the receiver is actually accepting the signals. Nevertheless, a slight drift of position over a long period can lead to an accident.

It is, hard to spoof a military GPS as it contains an encrypted binary code, the Y-code. This code is changed millions of times every second, not repeating for a period of at least a week. It is nearly impossible to generate it without having the actual encryption key.[190] On the other hand it is much easier to spoof a civil GPS receiver because it uses the open C/A-code that can be found on a public interface. [191]

There are two ways of being protected against spoofing. The first and more effective one, is by using a GPS receiver that contains a Selective Availability Anti-Spoofing Module (SAASM), which means, that it uses the Y-code. Nevertheless, only government authorized users can acquire these devices. The second way, which is open to public use, is by using a multi-constellation receiver that uses signals from GPS, GLONASS, BeiDou and Galileo. It is much harder to spoof signals coming from all these different frequency transmitters.[192]

In 2011, Iran claimed to be responsible for making a Lockheed Martin drone crash in Iranian territory and, in January 2016, two U.S. Navy Patrol Boats entered the Iranian waters, being intercepted and captured. Investigation about these two cases is still in development, but it is believed that it could have been spoofing attempts that changed the track of the U.S.' drone and patrol boats.[193]

---

[189]Novatel, *Understanding the Difference Between Anti-Spoofing and Anti-Jamming*.

[190]*Ibidem.*

[191]*Ibidem.*

[192]*Ibidem.*

[193]Mark Psiaki, Todd Humphreys, *Protecting GPS From Spoofers Is Critical to the Future of Navigation*, http://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation, (accessed January 2017).

Then how is spoofing really done? On civilian receivers, as said before, it is easily achieved. Knowing the exact position, you will be at the start of the spoofing session, the process starts. On that position, it is possible to find out which satellites will be in view, based on the satellites' ephemeris data. Given that, the spoofer calculates each satellite's Pseudo Random Noise (PRN) code using formulas that are available on a public database. Then, the spoofer sends out signals with the same codes as the satellites in view, which are accepted by the receivers as being part of the strongest true GPS signals. Finally, the hardest part is to drown the true signals by increasing the spoofing power until the receiver accepts them. Nevertheless, it is important (for the system not to fail and for the attempt to be disguised) to not increase the signal's power too much. Once the spoofed signals attach to the receiver, it can be adjusted leaving the actual true GPS signals behind and forgotten.[194]

In 2012, one year after the Lockheed Martin drone's crash disaster, the U.S. Department of Homeland Security decided to test if it was possible to attack a helicopter drone. For that matter, The University of Texas, more specifically Professor Todd Humphreys and his research team, prepared a trial at the White Sands Missile Range. They managed to complete the task of making the helicopter drone land - and nearly crash in the sand - by spoofing the GPS signals. The spoofed GPS signals kept telling the drone that is was ascending, which made it correct its position by pointing towards land.

In 2013, again, the University of Texas and Professor Todd Humphreys, organized a spoofing trial involving the vessel White Rose of Drachs. "The purpose of the experiment was to measure the difficulty of carrying out a spoofing attack at sea and to determine how easily sensors in the ship's command room could identify the threat".[195] The trial took place 30 miles off the coast of Italy, while the vessel travelled from Monaco to Rhodes, in Greece. Two students managed to take control of the ship's navigation system by overpowering the GPS signals. There was no sound of alarms, which made the situation

[194]Mark Psiaki, Todd Humphreys.

[195]UTNews, "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea", 2013, https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea, (accessed January 2017).

seem normal. As the team had total control of the ship's navigation systems they managed to change its course. Nevertheless, all that was seen on the electronic chart was a straight-line due to the course corrections that were being made but, in reality, they were gradually pushing away the ship from its actual track. After all the manoeuvres, under the spoofing attack, had been made, the ship turned out to be hundreds of meters away from the supposed electronic chart track.[196]

[196]UTNews.

Chapter 3 – Methodology

3.1 Resilience analysis

According to the definitions of resilience that were previously referred, a resilience assessment was made to all the Organisations that were studied throughout this project.

In order to analyse if the Organisations (and systems they depend on or supply) being studied in this project are working towards resilience, the following concepts had to be considered:

- Reconceptualization[197] – Does the Organisation approach the system's design problem in anticipation? Does it consider the need to change?
- Studying what goes right[198] – Do they consider studying what we consider everyday as "just happens"?
- Cultivating requisite imagination[199] – Do they anticipate failure before it occurs?
- Developing new tools to develop and operate systems[200] – do they to develop tools to help the systems control and adapt themselves?
- Creating ways to monitor the development and occurrence of unforeseen situations[201] – do their systems make adjustments and respond to unforeseen situations?

[197]Christopher Nemeth, Erik Hollnagel, *Becoming Resilient*, *Resilience Engineering in Practice Volume 2*, Ashgate Publishing Limited, Farnham, 2014, p xiii.

[198]*Ibidem,* p xiii.

[199]*Ibidem,* p xiii.

[200]*Ibidem,* p xiv.

[201]*Ibidem,* p xv.

- Cultivating ways to visualize and foresee side effects[202] – Do they create ways for systems to show how they adapt? Do they consider the interaction between systems and how cascading events may occur?
- Promoting and using great design[203] – do they give importance to good design as it can mitigate several issues?
- Acknowledging and managing variability[204] – do they embrace non-linear approaches in order to explore how systems and networks adapt?

When we talk about system resilience it is, almost, inevitable to refer the Systems-Theoretic Accident Modelling and Processes (STAMP)[205] approach by Nancy Leveson. This model considers safety and resilience as control problems and, includes:

- Approaches to accident investigation/analysis;
- Hazard analysis;
- Accident prevention;
- Risk assessment;
- Risk management;

In the STAMP approach, accidents are seen, not only because of component malfunction, but also as results of improper processes due to[206]:

- Interactions between societies, people or organisational structures;
- Engineering activities;
- System components;
- Poor safety control on the system's creation, design, construction and operation.

---

[202]Christopher Nemeth, Erik Hollnagel, p xv.

[203]*Ibidem*, p xv.

[204]*Ibidem,* p xvi.

[205]Erik Hollnagel, David Woods, Nancy Leveson, *Resilience Engineering, Concepts and Precepts*, Ashgate Publishing Limited, Farnham, 2006, pp 96-107.

[206]*Ibidem*, p 97.

This model, inspired the data analysis of this project, as it offers theoretical foundation to develop important tools for project managers in order to assist them in risk management and building resilient systems. The three STAMP fundamental concepts can be seen on Figure 6 below. The absence of control on these concepts can lead to accidents.

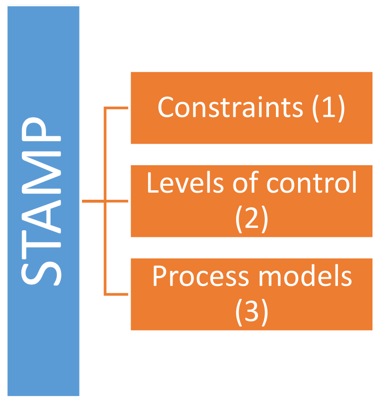


Figure 6 - STAMP fundamental concepts[207]

(1) Constraints – systems are viewed as hierarchic structures, in which, each above level implies constraints to the level below. “Accidents result from inadequate enforcement of constraints on behaviour (e.g., the physical system, engineering design, management, and regulatory behaviour)”[208].

(2) Levels of control – between these levels need to be communication channels in order to send the constraints information to the levels below and a measuring channel for sending feedback (status reports, risk assessments, etc.).

(3) Process models – must contain the system’s current state; relationship required between the different variables; and in which ways the process can change. Accidents often occur when there is a discrepancy between the process model and the actual process state.

[207]Nancy Leveson, *A New Accident Model for Engineering Safer Systems*, Massachusetts Institute of Technology, Massachusetts, 2004, pp 12-13.

[208]Erik Hollnagel, David Woods, Nancy Leveson, pp 99.

This approach considers the following procedures and advices (that are implied in Leveson's theory)[209]:

- Definition of the task that is being analysed (define the objective and boundaries);
- Data collection (ex: accident and enquiry reports);
- Construction of the Hierarchical control structure (based on the data collection process);
- Bad control analysis (identification of the control failures);
- Review and Analysis (creation of a report).

STAMP makes it possible to analyse hazards and create techniques in order to prevent them when accidents are not – only - a consequence of component failure. These techniques lead to building more resilient systems as they are more prepared against operation-error accidents, human or organisational-caused accidents.

In this project, the resilience assessment to the organisations was made through data collection by Interviews (Online questionnaire and Open Interview) and, in the Portuguese Navy, more specifically, through GPS Jamming Trials - considered as a possible "accident".

3.2 Stakeholder analysis

In order to perform a stakeholder analysis and find out which individuals or organisations depend on PNT systems for achieving their daily objectives and organisational goals, an American study[210] led by RAND Corporation was used. This study includes a description of the US' GPS Stakeholders which eased the process of determining the Portuguese GNSS stakeholders. Nevertheless, Portugal does not have exactly the

[209] Nancy Leveson, pp 25-30.

[210] Scott Pace, *et al.*, *The Global Positioning System: Assessing National Policies*, California, RAND Corporation, 1995, pp 11-44.

same organisations or individuals, which required an adaptation process and the creation of selection criteria. The stakeholders were chosen throughout the following steps[211]:

- 1st step: Identifying which is the main theme: PNT Systems;
- 2nd Step: Defining which groups or individuals depend or share interest in this theme: Users (Positioning, Navigation and Timing); GNSS Services Suppliers; GNSS-dependent Services Suppliers, Academia, Investigation, Control and Vigilance Authorities; and Regulating Authorities;
- 3rd step: Identify how many individuals or organisations exist according to the previously defined groups.

Naturally, a stakeholder analysis should answer the following questions[212]:

- What are the current and future interest of these stakeholders in the use and management of this theme?
- How do they use it?
- How do they benefit from it?
- What are their rights and responsibilities towards the main theme?
- Which are the networks and organisations they take part in?
- How willingly are they to participate in this theme’s management?
- Which are the human, technical and financial resources that they are willing to give out for managing this theme?

The final Stakeholder groups that were identified were:

- Users (for Positioning purposes);
- Users (for Navigation purposes);
- Users (for Timing reference purposes);
- Investigation;
- Academia;

[211]Károly Futaki, *Danube Flood risk Project, Stakeholder Selection Strategy,* VKKI, Budapest, 2010, p 9.

[212]Károly Futaki, p 11.

- GNSS Services Suppliers;
- GNSS-dependent Services Suppliers;
- Regulating Authorities;
- Control and Vigilance Authorities.

Also, in order to identify, which stakeholders were indispensable for the development of this project, an analysis of the Potential stakeholders[213] was made, according to their importance, and can be seen on Table 3 below.

Primary Stakeholders	Secondary Stakeholders	Key Stakeholders
• GNSS-dependent Services Suppliers • GNSS Services Suppliers	• Academia • Users	• Regulating Authorities • Control and Vigilance Authorities

Table 3 – Primary, Secondary and Key Stakeholders

Primary Stakeholders are considered "Beneficiaries or targets of the effort"[214]; Secondary Stakeholders are considered "the ones whose jobs or lives might be affected by the process or results of the effort"[215]; Key stakeholders are "Government officials and Policy makers"[216].

After the Stakeholders Identification was concluded, a research of these representatives in Portugal was made and, then, Organisations and Individuals were contacted through e-mail – APPENDIX A. The ones who replied were asked to answer to an online questionnaire and an Open Interview.

For the Online Questionnaire, Google Forms was used as a web open-source application for data collection. The data analysis nevertheless, could only be statistically

[213] Phil Rabinowitz, *Section 8. Identifying and Analyzing Stakeholders and Their Interests*, http://ctb.ku.edu/en/table-of-contents/participation/encouraging-involvement/identify-stakeholders/main, (accessed June 2017).

[214] *Ibidem.*

[215] *Ibidem.*

[216] *Ibidem.*

analysed by groups of stakeholders, as some groups had only one representative stakeholder. The quantitative analysis of the Online Questionnaire responses was made in Microsoft Excel, and results presented in several diagrams.

At last, the Open Interview, through voice recording, was analysed through the MAXQDA 12 software that makes it possible to code pre-defined words or phrases that are considered important. When all the interviews were coded, it was possible to see the elements that were shared between each Organisation - or individual representing an Organisation - and possible solutions that were presented – and sometimes similar. These results can, also, be seen in Chapter 4.

3.3 Resilience in operations – Jamming Trial

In order to assess the PNT resilience in the Portuguese Navy, three jamming trials were performed aboard a Portuguese Warship. These trials were theoretically based on two previous jamming trials performed by the GLA that - described in Chapter 2. They helped to predict what could happen, in the worst perspective.

For this project's trials two distinct models of jammers were acquired for redundancy – as there was no guarantee any of them would work. During the trials, data was extracted from the Ship's Master device directly to a computer, and was parsed with open sourced script from http://freenmea.net/dashboard#/files,.

Initially, a schedule was elaborated in order to be compatible with the ship's operational commitment. The schedule can be seen on Table 4 below.

Phases	Objectives
Preparation (In harbour)	• Investigate previous international Trials; • Visiting the ship in order to evaluate what systems it had and test data extraction to a personal computer; • Material preparation (video recorder, jamming devices, Spectrum Analyzer (R&S FSH3), Computer, R232 Cable); • Briefing for the Ship's Commander in order to explain the objectives of the study and Trial
1st Trial	• Test the crew's reaction in a hazardous environment (alarms sounding on the bridge and system's unavailability); • Evaluate systems' reactions • Are there any back-ups?
2nd Trial	• No surprise factor – after the first trial the crew already knew what was happening; • Systems' reactions to GPS information denial; • Video record Procedures for digital proof;
3rd Trial	• No surprise factor anymore - after the first trial the crew already knew what was happening; • Systems' reactions to GPS information denial; • Video record Procedures for digital proof;

Table 4 - Trial Schedule

Nevertheless, there was one difference between the jamming trial led on this project and the ones led by the GLA: the "surprise factor". This item is very important for evaluating part of the Organisation's resilience and could not be tested. The fact that the three jamming trials were performed during the same period aboard made it impossible, as the crew members soon realized what was happening.

In order to perform a vulnerability assessment, an event sheet was created in order to keep redundancy on data recording (and register other details that could not be recorded). It was used in every trial and can be seen on Figure 7.

Sea Trial					
Date					
Trial Number					
ECDIS on alarm?	Yes	No			
Jammer's Position			Nº compartments to exterior		
Operator detected GPS alarm?	Yes	No	Time:		
Giro Failed?	Yes	No			
ARPA failed?	Yes	No			
AIS failed?	Yes	No			
GMDSS on alarm?	Sim	Não			
Officer-on-watch adopted any procedure?	Yes	No	Time		Procedure
Was the Technical Service informed?	Yes	No	Time		
Are there any Ships in the area?	Yes	No			
If yes, were they informed?	Yes	No			
Observations					

Figure 7 - Trial event sheet

Chapter 4 –Results

4.1 Portuguese PNT Stakeholders point of view and needs

4.1.1 Online Questionnaire

In the stakeholder enquiry through the online questionnaire, 15 questions were chosen (2 out of these 15 questions referred to demographic data to identify which organisation they worked for or who they were). Personal information was treated confidentially and was not used for any statistic purpose. The template can be found in APPENDIX B.

The online questionnaires were analysed by grouping the stakeholders, according to their own classification (some stakeholders considered themselves to be part of more than one group).

The Investigation stakeholders believe they are quite dependent on GNSS (mean=7.5 on a scale from 0 to 10); largely dependent on GNSS for Positioning (mean=8.75 on a scale from 0 to 10); averagely dependent on GNSS for Navigation (mean=5.63 on a scale from 0 to 10) and even less dependent for timing information (mean=4.88 on a scale from 0 to 10). Also, they do not consider their organisation totally prepared in case of GNSS unavailability (mean=3.13 on a scale from 0 to 10) but, a large part of them, stated that their organisations have backup systems in case of GNSS unavailability (62.5%). The parameters that the investigation stakeholders considered vital for responding to their daily service needs are Precision, Coverage, Accuracy, Availability and Integrity (14.6% each). Nevertheless, GPS is not the only system they use. Other systems were referred: DGPS, EGNOS, GALILEO, WAAS, GLONASS, BeiDou, PPP, even though they consider rather important for other GPS complementing systems to be adopted and implemented in Portugal (mean=8 on a scale from 0 to 10). When asked their opinion about what solution should be implemented to augment GPS' performance, the most common answer was the implementation of local systems (ex: Pseudolites) (62.5%).

At last, these stakeholders believe that the Portuguese population's knowledge of PNT systems is below average (mean=3.63 on a scale from 0 to 10).

The users (for Navigation purposes) believe they are quite dependent on GNSS (mean=7.44 on a scale from 0 to 10); largely dependent for Positioning (mean=8.25 on a scale from 0 to 10); considerably dependent on GNSS for Navigation (mean=6.56 on a scale from 0 to 10) and also on GNSS for timing information (mean=6.88 on a scale from 0 to 10). Also, they consider their organisation averagely prepared in case of GNSS unavailability (mean=5.13 on a scale from 0 to 10) and, most of them, stated that their organisations have backup systems in case of GNSS unavailability (62.5%). The parameter that they considered vital for responding to their daily service needs is Availability (15%). Nevertheless, GPS is not the only system they use. Other systems and services were referred: DGPS, EGNOS, GALILEO, WAAS, GLONASS; though they consider rather important for other GPS complementing systems to be adopted and implemented in Portugal (mean=8.06 on a scale from 0 to 10). When asked their opinion about what solution should be implemented to augment GPS' performance, the most common answer was the implementation of local systems (ex: Pseudolites) (37.5%). At last, these stakeholders believe that the Portuguese population's knowledge of PNT systems is below average (mean=3.43 on a scale from 0 to 10).

The users (for Positioning purposes) stakeholders believe they are quite dependent on GNSS (mean=7.44 on a scale from 0 to 10); largely dependent for Positioning (mean=8.11 on a scale from 0 to 10); averagely dependent on GNSS for Navigation (mean=5.76 on a scale from 0 to 10) and also considerably dependent on GNSS for timing information (mean=6.11 on a scale from 0 to 10). Also, they consider their organisation averagely prepared in case of GNSS unavailability (mean=5.05 on a scale from 0 to 10) but, most of them, stated that their organisations have backup systems in case of GNSS unavailability (70%). The parameter that they considered vital for responding to their daily service needs is Availability (15.7%). Nevertheless, GPS is not the only system they use. Other systems and services were referred: DGPS, EGNOS, GALILEO, WAAS, GLONASS; even though they consider rather important for other GPS complementing systems to be adopted and implemented in Portugal (mean=7.30 on a scale from 0 to 10). When asked their opinion about what solution should be implemented to augment GPS' performance, the most common answer was the implementation of local systems (ex: Pseudolites) (35.3%). At last, they believe that the Portuguese population's knowledge of PNT systems is below average (mean=3.47 on a scale from 0 to 10).

The users (for Time Reference purposes) believe they are dependent on GNSS (mean=7 on a scale from 0 to 10); largely dependent for Positioning (mean=7.8 on a scale from 0 to 10); considerably dependent on GNSS for Navigation (mean=6.2 on a scale from 0 to 10) and largely dependent for timing information (mean=7.5 on a scale from 0 to 10). Also, they consider their organisation averagely prepared in case of GNSS unavailability (mean=5.4 on a scale from 0 to 10) but most of them stated that their organisation has backup systems in case of GNSS unavailability (70%). The parameter that they considered vital for responding to their daily service needs is Availability (17%). Nevertheless, GPS is not the only system they use. Other systems and services were referred: DGPS, EGNOS, GALILEO, GLONASS, WAAS; even though they consider rather important for other GPS complementing systems to be adopted and implemented in Portugal (mean=7.6 on a scale from 0 to 10). When asked their opinion about what solution should be implemented to augment GPS' performance, the most common answer was the adoption and training of complementary navigation methods (ex: Celestial Navigation) (50%). At last, these stakeholders believe that the Portuguese population's knowledge of PNT systems is below average (mean=3.9 on a scale from 0 to 10).

The Control and Vigilance Authorities consider themselves dependent on GNSS (mean=7.6 on a scale from 0 to 10); largely dependent for Positioning (mean=7.8 on a scale from 0 to 10), largely dependent on GNSS for Navigation (mean=7 on a scale from 0 to 10) and for timing information (mean=7.6 on a scale from 0 to 10). Also, they consider their organisation prepared in case of GNSS unavailability (mean=8 on a scale from 0 to 10) but, all of them, stated that their organisation has backup systems in case of GNSS unavailability (100%). The parameter that they considered vital for responding to their daily service needs is Precision, Accuracy and Availability (14.8% each). Nevertheless, GPS is not the only system they use. Other systems and services were referred: DGPS, EGNOS, GALILEO, GLONASS, AIS; even though they consider rather important for other GPS complementing systems to be adopted and implemented in Portugal (mean=7.8 on a scale from 0 to 10). When asked their opinion about what solution should be implemented to augment GPS' performance, the most common answer was the adoption and training of complementary navigation methods (ex: Celestial Navigation) and investment in regional and local differential systems (ex: DGPS, WAAS, etc.) (40%, each). At last, these stakeholders believe that the Portuguese population's knowledge of PNT systems is way below average (mean=1.8 on a scale from 0 to 10).

The Academia Stakeholders believe they are dependent on GNSS (mean=8 on a scale from 0 to 10), largely dependent for Positioning (mean=9 on a scale from 0 to 10), averagely dependent on GNSS for Navigation (mean=5.25 on a scale from 0 to 10) and a little less dependent for timing information (mean=4.75 on a scale from 0 to 10). Also, they consider their organisations considerably prepared in case of GNSS unavailability (mean=6 on a scale from 0 to 10) but, all of them, stated that their organisations have backup systems in case of GNSS unavailability (100%). The parameter that they considered vital for responding to their daily service needs is Continuity, Integrity, Availability and Accuracy (14.3% each). Nevertheless, GPS is not the only system they use. Other systems and services were referred: DGPS, EGNOS, GALILEO, GLONASS, WAAS; even though they consider rather important for other GPS complementing systems to be adopted and implemented in Portugal (mean=8 on a scale from 0 to 10). When asked their opinion about what solution should be implemented to augment GPS' performance, the most common answer was the use of local systems (ex: Pseudolites) (50%). At last, these stakeholders believe that the Portuguese population's knowledge of PNT systems is way below average (mean=2.25 on a scale from 0 to 10).

The GNSS-dependent services suppliers consider themselves GNSS-dependent (mean=8.5 on a scale from 0 to 10), largely dependent for Positioning (mean=9.5 on a scale from 0 to 10), considerably dependent on GNSS for Navigation (mean=6.75 on a scale from 0 to 10) and also for timing information (mean=6.25 on a scale from 0 to 10).

Also, they consider their organisations averagely prepared in case of GNSS unavailability (mean=5.25 on a scale from 0 to 10) and, most of them, stated that their organisations have backup systems in case of GNSS unavailability (75%). The parameter that they considered vital for responding to their daily service needs is Availability and Continuity (16% each). Nevertheless, GPS is not the only system they use. Other systems and services were referred: DGPS, EGNOS, GALILEO, GLONASS, WAAS, BeiDou, PPP; even though they consider rather important for other GPS complementing systems to be adopted and implemented in Portugal (mean=7.25 on a scale from 0 to 10). When asked their opinion about what solution should be implemented to augment GPS' performance, no conclusions can be taken as all the answers were different. At last, these stakeholders believe that the Portuguese population's knowledge of PNT systems is below average (mean=3.25 on a scale from 0 to 10).

The GNSS services suppliers, included in this study, believe they are dependent on GNSS (mean=8.4 on a scale from 0 to 10), largely dependent for Positioning (mean=8.8 on a scale from 0 to 10), considerably dependent on GNSS for Navigation (mean=6.8 on a scale from 0 to 10) and also for timing information (mean=6 on a scale from 0 to 10). Also, they consider their organisation's preparation below average in case of GNSS unavailability (mean=4.4 on a scale from 0 to 10) but, most of them, stated that their organisations have backup systems in case of GNSS unavailability (60%). The parameter they considered vital for responding to their daily service needs is Availability and Integrity (16.7% each). Nevertheless, GPS is not the only system they use. Other systems and services were referred: DGPS, EGNOS, GALILEO, GLONASS, WAAS, BeiDou, PPP; even though they consider rather important for other GPS complementing systems to be adopted and implemented in Portugal (mean=7.4 on a scale from 0 to 10). When asked their opinion about what solution should be implemented to augment GPS' performance, the most common answer was the implementation of local systems, like "Pseudolites" (40%). At last, these stakeholders believe that the Portuguese population's knowledge of PNT systems is below average (mean=3.6 on a scale from 0 to 10).

Only one Regulating Authority; Cartography Producer; Web Applications Developer; Security; and Geodesy, Topography and Hydrography, stakeholders were interviewed, which means, no conclusions can be stated.

As general results, including all stakeholders, it could be stated most consider themselves GNSS dependent; mostly used GNSS systems are GPS, DGPS, GLONASS, GALILEO AND EGNOS; most of the Stakeholders consider themselves quite dependent to GNSS but, averagely prepared in case of GNSS unavailability. This can be seen on Figure 8 below. The remaining graphs that were used for results presented in this chapter can be found in APPENDIX C.

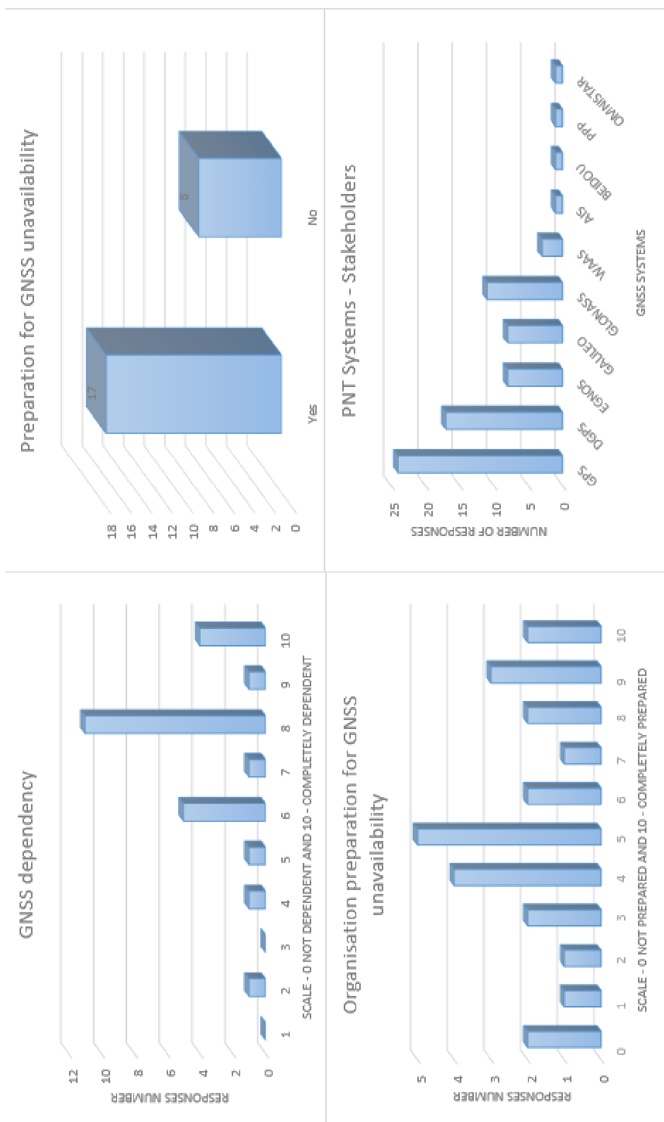


Figure 8 - General questionnaire results

4.1.2 Open interview

All the interviews made were transcript and coded. The most common topics, shared by nearly all the interviewees, can be seen on Figure 9. After the most common topics were identified, a Mind Map was created using the Software VUE in order to associate these topics with the groups of stakeholders that referred them. The Full Mind Map can be found on APPENDIX E. Then, an analysis of each most common topic was made in order to take conclusions from the open interviews.

Código	Segmentos codificados de todos os documentos	Data de criação	% Segmentos codificados de todos os documentos	Documentos
Eficiency	3	03/06/2017 17:24	0.96	1
Resilience	7	03/06/2017 17:23	2.25	2
Redundancy	8	03/06/2017 17:07	2.57	7
Costs	12	03/06/2017 17:08	3.86	6
Necessary GNSS characteristics	12	03/06/2017 17:02	3.86	7
Vulnerability	23	03/06/2017 17:06	7.40	9
Solutions presented	70	03/06/2017 17:04	22.51	18
GNSS dependency	73	03/06/2017 17:01	23.47	18
Alternatives	103	03/06/2017 17:03	33.12	21

Figure 9 - Commons topics – Open Interviews (MAXQDA12)

The most common topics that were referred by all the stakeholders interviewed, were:

- Efficiency;
- Resilience;
- Redundancy;
- Costs;
- Necessary GNSS characteristics;
- Vulnerability;
- Solutions presented;
- GNSS dependency;
- Alternatives.

Several solutions and alternatives were presented and can be seen on Figure 10 below. Other screenshots from the Mind Map - based on the results of the Personal

Interviews including which Stakeholders referred each topic, how many of them did and what solutions and alternatives did they present - can be seen in APPENDIX F.

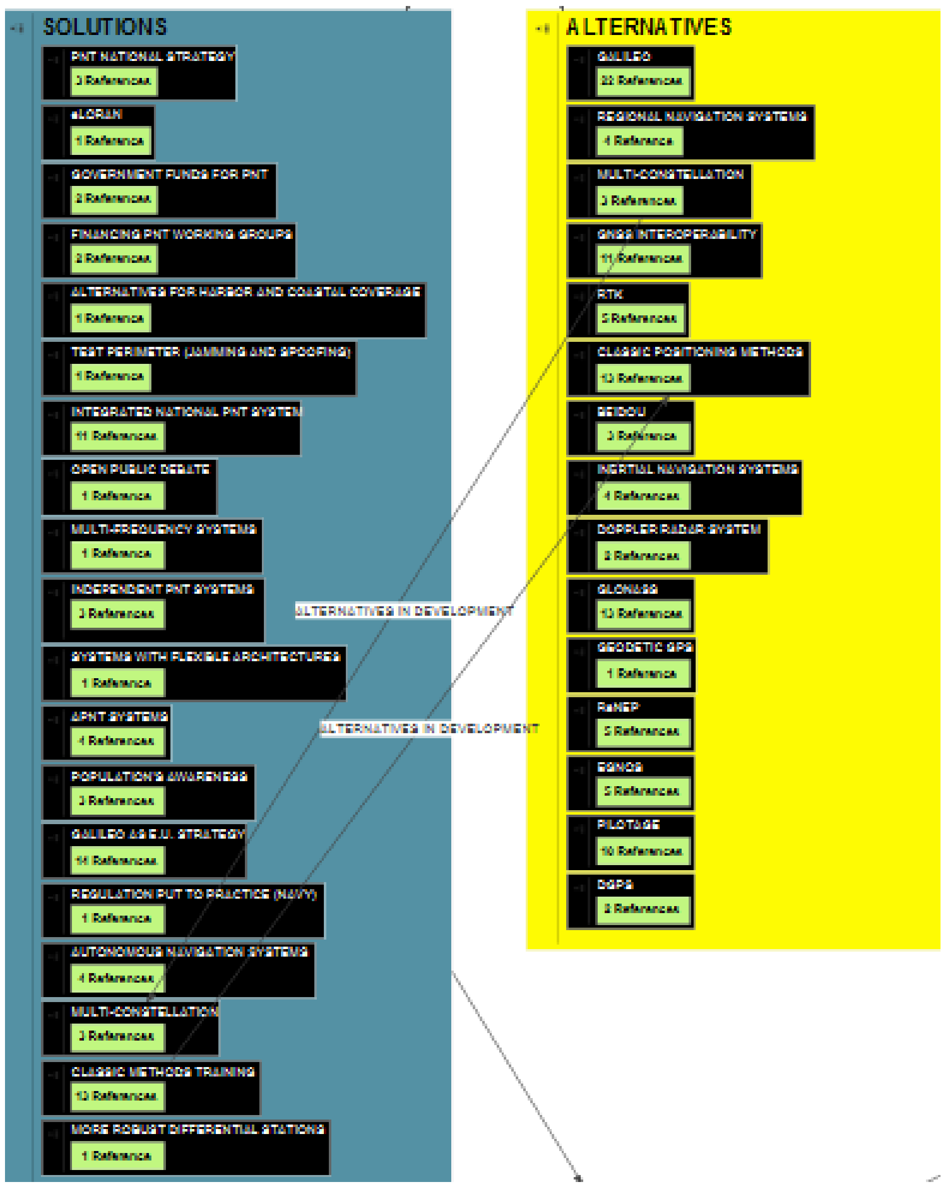


Figure 10 - Topics 'Solutions' and ' Alternatives'

4.2 Jamming Trial

During the three jamming trials, when the Jamming signal was powerful enough, due to the proximity to the GPS antenna, several equipment failed. This can be shown and described on Table 5 and pictures are shown in APPENDIX G.

EQUIPMENT	MESSAGE	DESCRIPTION
AIS	"No sensor position in use" Figure 60 (APPENDIX G)	No positioning sensor was available.
AIS	"UTC Sync Invalid" Figure 61 (APPENDIX G)	AIS could not synchronize it's time with GPS due to its unavailability
ECDIS	"No Fix" Figure 62 (APPENDIX G) "UTC AIS: sync invalid" Figure 63 (APPENDIX G)	No positioning sources. AIS could not synchronize it's time with GPS due to its unavailability
GPS	"No Fix" Figure 65 (APPENDIX G)	No positioning sources.
ARPA Radar	"Position: Loss of Position GPS1" Figure 64 (APPENDIX G)	No positioning sources.
Sailor VHF	"Cannot acquire synchronization at the satellite channel. Please initiate a scan" Figure 66 (APPENDIX G)	Sailor VHF could not find any GPS Satellites.
Sailor VHF	"Hardware Problems. Distress button failure. Distress button may no longer work" Figure 67 (APPENDIX G)	Distress button could not work without any positioning.

Table 5 - Equipment failure during Jamming Trials

The following figures show, the results that were obtained during the First, Second and Third Jamming Trials. The Latitude, Longitude and Speed Variation was null in the periods where the jammers were effective (as there was no positioning or speed data). The graphs show the variation in meters per minute, for the Latitude and Longitude and, in knots per minutes, for Speed.

4.2.1 First Trial

For this particular trial, vertical bars are shown when there was no positioning, navigation or timing information (when the latitude, longitude or speed variation was zero), which means that the position at some points was null (Position 2 – Position 1 = 0). This means that at these points - where the vertical bars were shown and there is no position or speed variation - the jammers were on.

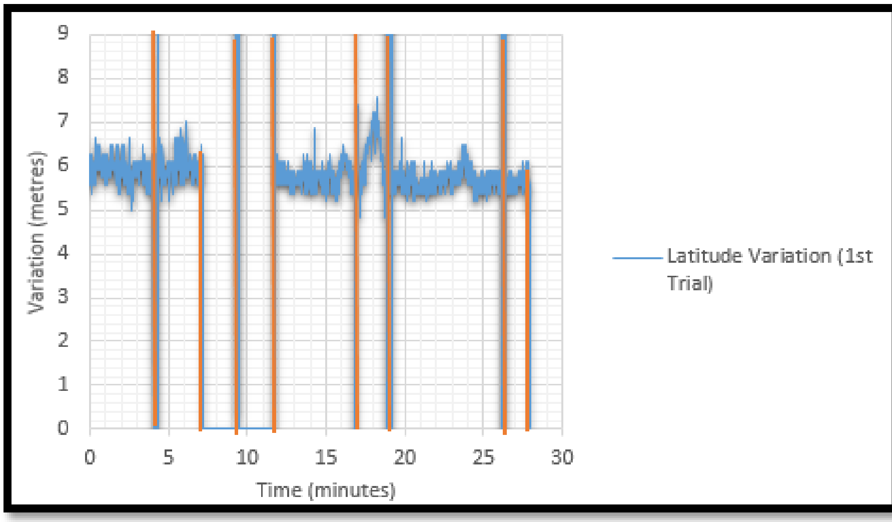


Figure 11 - Latitude Variation (1st Trial)

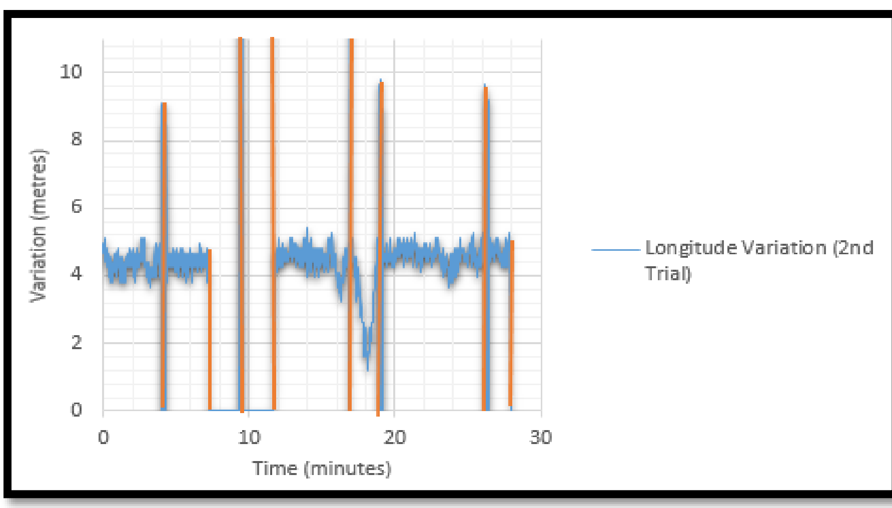


Figure 12 - Longitude Variation (1st Trial)

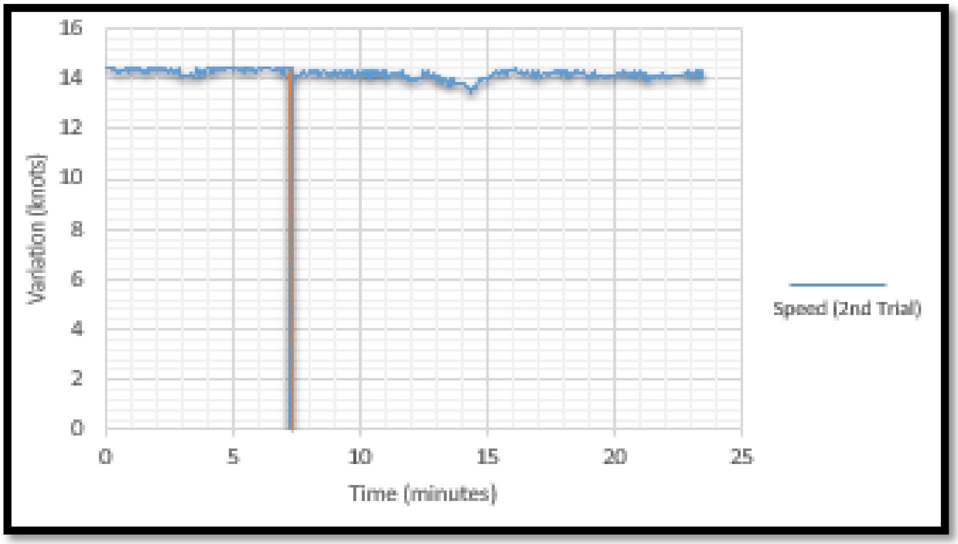


Figure 13 - Speed Variation (1st Trial)

4.2.2 Second Trial

Similar to the first trial, vertical bars are shown when there was no positioning, navigation or timing information (when the latitude, longitude or speed variation was zero), which means that the position at some points was null (Position 2 – Position 1 = 0). This means that at these points - where the vertical bars were shown and there is no position or speed variation - the jammers were on. Nevertheless this test was not as conclusive as the first - due to some values not being as regular as in the first trial as the naval unit was anchoring in harbour.

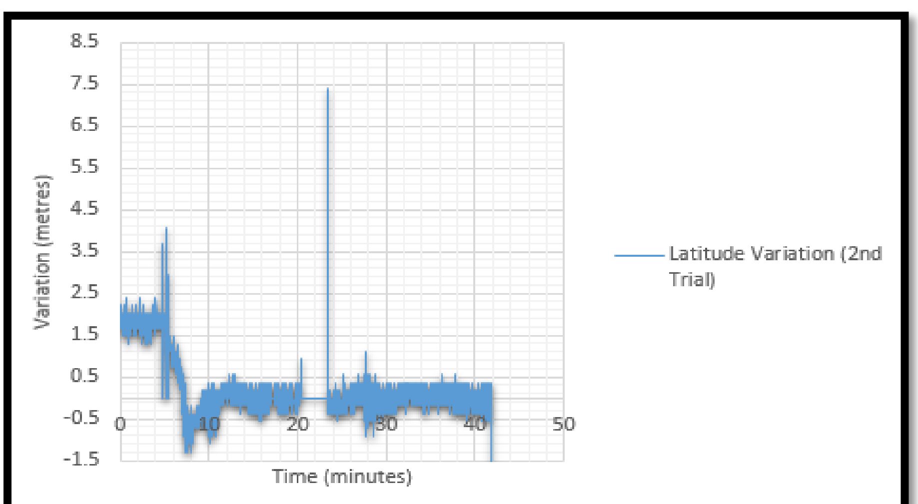


Figure 14 - Latitude Variation (2nd Trial)

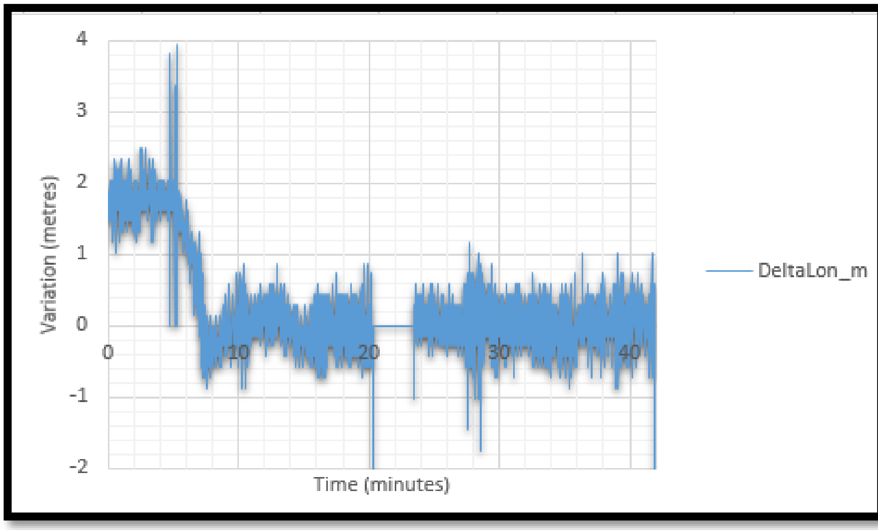


Figure 15 - Longitude Variation (2nd Trial)

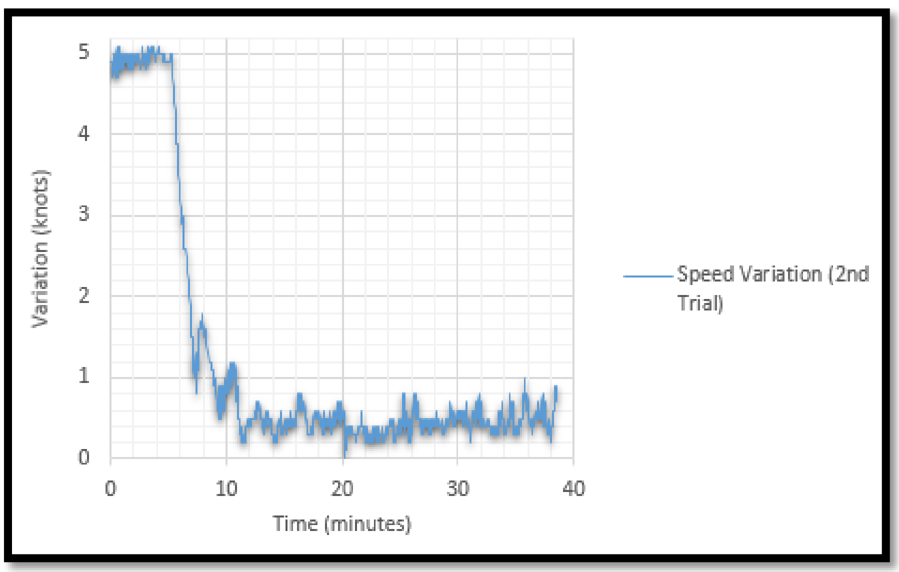


Figure 16 - Speed Variation (2nd Trial)

4.2.3 Third Trial

Similar to the second trial, this test was not as conclusive as the first due to some values not being as regular as in the first trial – the naval unit was anchoring in harbour, leading to some unexplainable values and small positioning and speed variation.

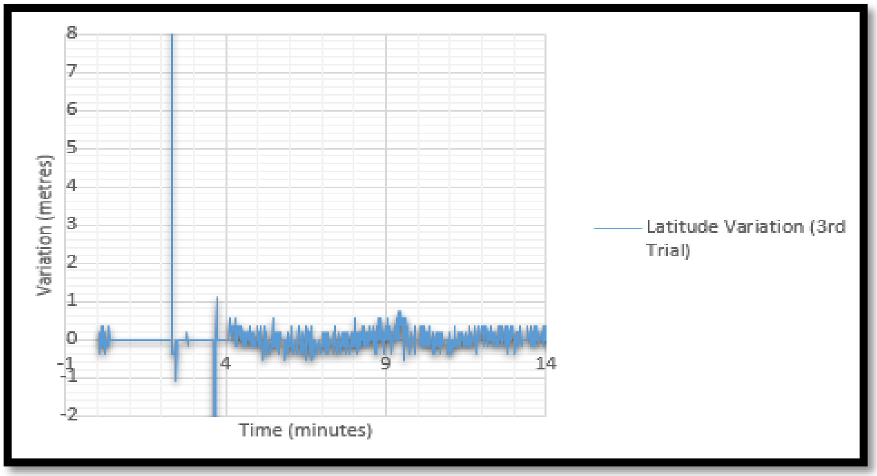


Figure 17 - Latitude Variation (3rd Trial)

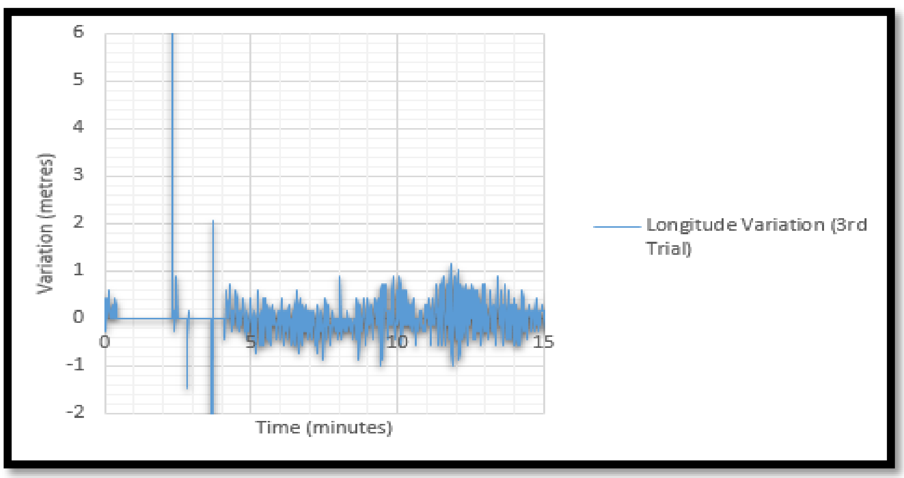


Figure 18 - Longitude Variation (3rd Trial)

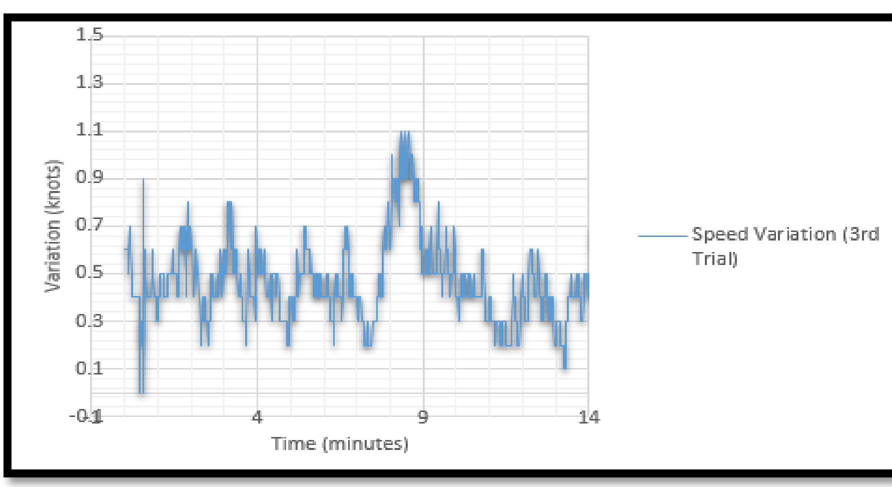


Figure 19 - Speed Variation (3rd Trial)

4.2.4 Spectrum Analyzer

The Spectrum Analyzer, R&S FSH3, was used in order to see the difference between a “no-jamming” period and the jamming periods, in terms of the frequencies. This made it possible to see that during the jamming periods the SNR was much higher than during the no-jamming periods. These intense signals – transmitted by the jammer – operating in the GPS L1 band, “drowned” the true GPS signals and lead to no PNT information, during the three trials. This can be seen in Figures 20 and 21, using the J242-G and J220-B model, at different distances from the ship’s GPS antenna.

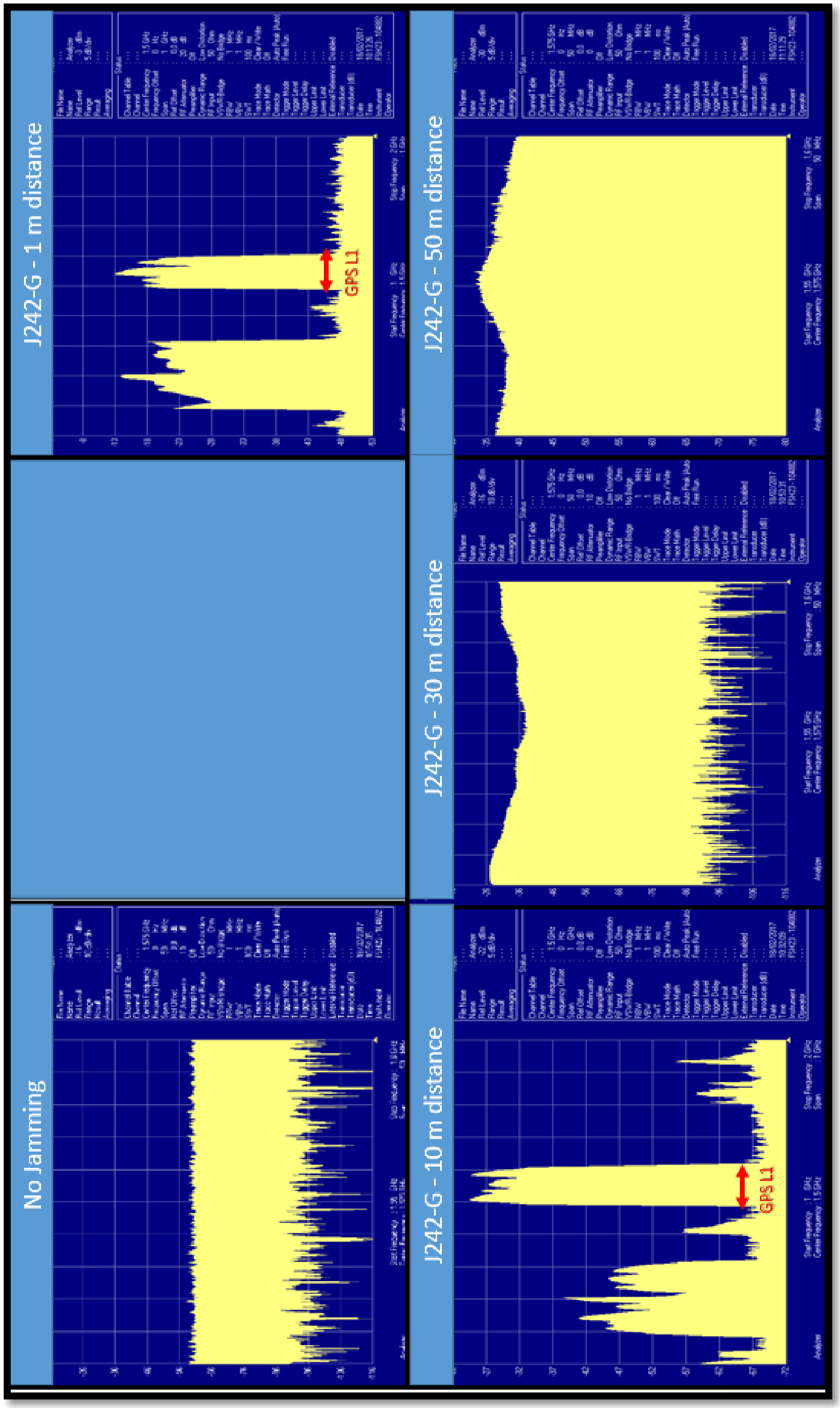


Figure 20 - Spectrum Analyzer (J242-G model)

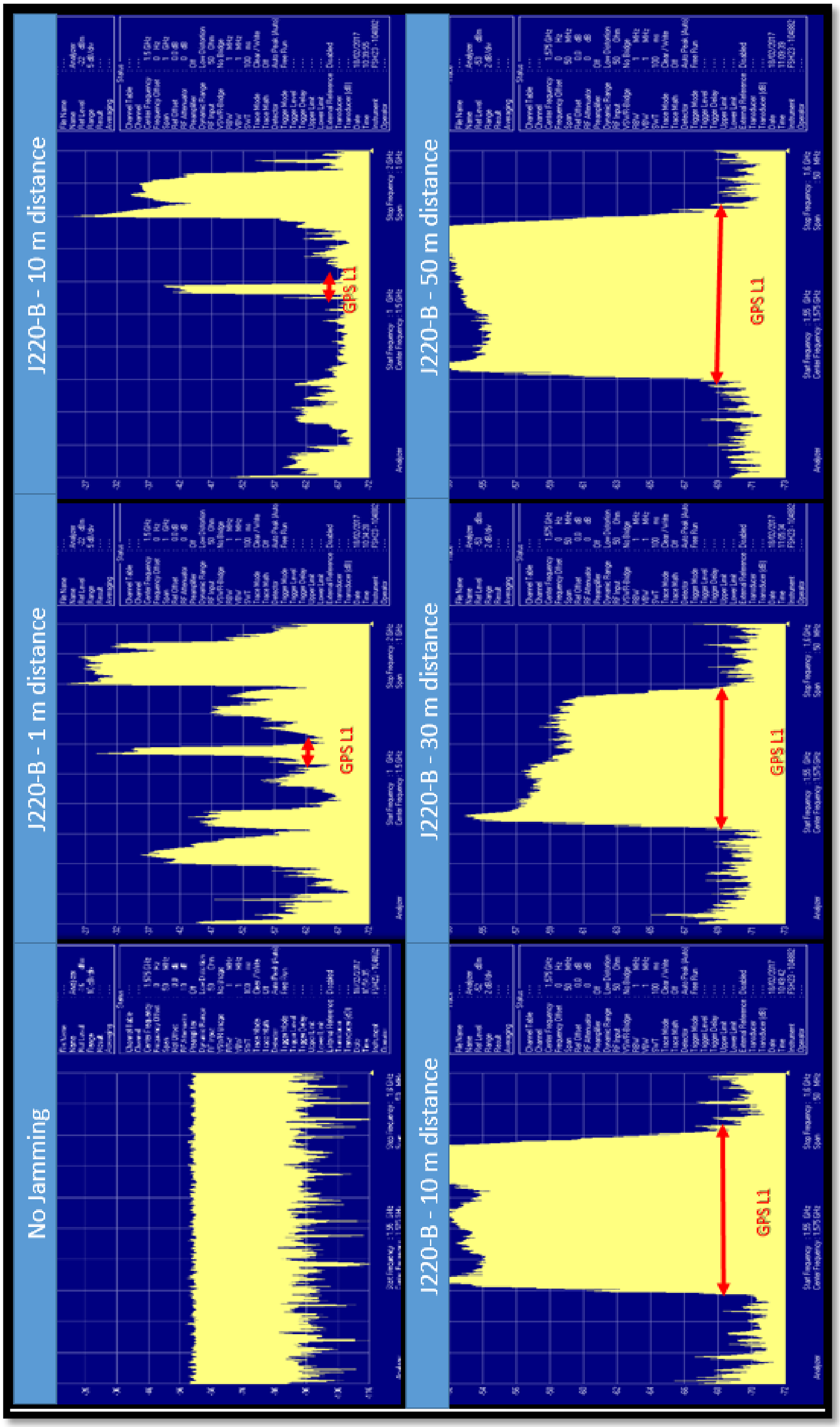


Figure 21 - Spectrum Analyzer (J220-B model)

Chapter 5 – Analysis

5.1 Portuguese PNT stakeholders

Portuguese Organisations believe, generally, in the need of Availability in PNT services and, it should be a requirement for a resilient PNT system. There should be a higher investment in implementing local systems, such as Pseudolites or training complementary navigational methods, like Celestial Navigation. Most of the organisations have backup systems in case of GNSS unavailability, but consider themselves GNSS dependent in order to maintain normal service functioning. The previous results can be seen on Figure 22 below.

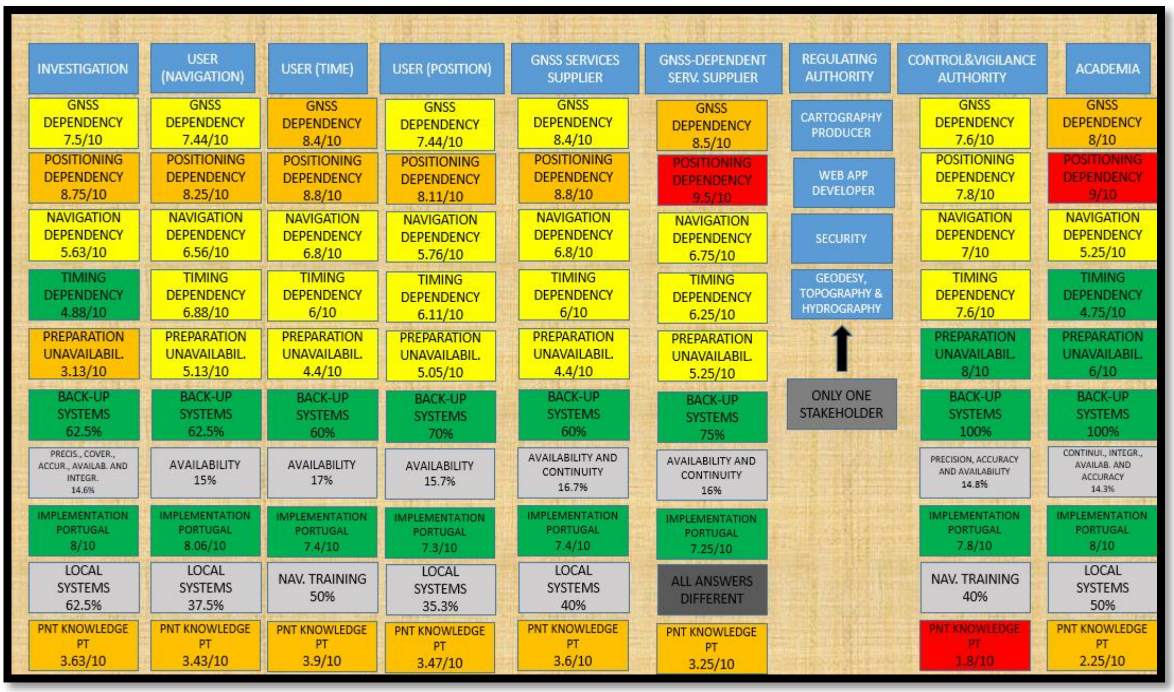


Figure 22 - Questionnaire results

The personal interviews helped comparing the different stakeholder's groups and analyse all the similar elements that they share, in a more complex way.

Two concept were highlighted by an Academia Stakeholder during the Personal Interview: Efficiency and Resilience. He believes that one of the problems the future generation will be confronted with is the lack of the resources that are used to produce components for electronic systems like satellite vehicles. This means, in this stakeholder's opinion, countries may choose to adopt a resilient or an efficient strategy, which he explained in the following way: "if a country has a saving economic strategy with low investment, in a crisis situation, there will be a saved fund ready to be used. This is resilience. The result will be slow economic growth but, also, high capacity of recovering in a hazardous situation. In the efficiency strategy, the aim is to reduce the stock and increase the investment. This leads to a more dynamic and growing economy, disregarding the capacity to recover in an unpredictable event."[217]

The concept of Redundancy was also dominant, as the Stakeholders believe there should always be a redundant back-up system. It can be, per example, having two GPS receivers, having GPS and a Maritime Inertial Navigation System or, simply, using Classic Methods (ex: Celestial Navigation), that are still being used and do not depend on any signal reception or advanced technology.

In general, most of the GNSS' performances parameters were referred like the importance of Precision, Accuracy, Integrity, Availability, Continuity, Robustness, Coverage and Reliability for the quality of their products/services or, in some cases, personal safety (for example during flight procedures). "In open-sea there is not a necessity, as high as in coastal waters, of accuracy and reliability"[218]. It was also stated that constellations should be designed in order to cover as much area as possible and for satellites to have the longest useful lifetime possible: "When all the satellites (GALILEO) are in orbit, there will be permanent global coverage"[219].

Another topic referred was the importance of costs. "There should be Portuguese alternatives to GNSS but, are the costs worth it?"[220] Most of the stakeholders that referred this topic believe that, due to the Portuguese socio-economical context, it is not crucial and favourable to invest in this area. Rather than the initial investment there is, still, the maintenance component which involves high periodic costs. "What I can see in a near

[217]Translated by the Author.
[218]Translated by the Author.
[219]Translated by the Author.
[220]Translated by the Author.

future is significant maintenance cost, as stations will need maintenance and updates. Who is going to pay for this?"[221]

Vulnerability was also a topic constantly being repeated. We are vulnerable if we depend, only, of American (GPS) and Russian (GLONASS) GNSS. Critical and emergency services do not use GPS as a primary method due to its vulnerability and possible unavailability (ex: INEM; Stock Exchange, etc.). "Something that really depends on time synchronism is the Stock Exchange. If it collapses it's over. A nanosecond can be enough"[222]. In a crisis situation, the primary systems tend to fail first and, it is in these types of situations, that we can see how vulnerable we are. "If everything fails and there is no knowledge, I cannot work"[223].

Another interesting fact is that some stakeholders believe we are vulnerable just by having to go back to traditional methods if all GNSS fail. "It is always harder to go back"[224]. Nevertheless, some specified that it is not trivial that all systems should fail at the same time and, in some systems, a temporary fail will not have any impact and may, even, be detected and automatically corrected.

According to the Methodology used for this project for analysing Organisations, some important elements were: Reconceptualization; Studying what goes right; cultivating requisite imagination; and acknowledging and managing variability[225]. For this mean, several solutions, were presented by the interviewees for a resilient Portuguese PNT future:

- Implement a PNT National Strategy;
- Government financing on national PNT projects and working groups;
- Government funding and creation of a directive structure to promote PNT research in Portugal (create a National PNT Council);

[221]Translated by the Author.
[222]Translated by the Author.
[223]Translated by the Author.
[224]Translated by the Author.
[225]Christopher Nemeth, Erik Hollnagel, pp xiii-xv.

- Create a Jamming and Spoofing Testing Perimeter (like the U.S.' White Sands Missile Range) for GNSS researchers, developers and military use;
- Population's awareness of the GNSS' flaws;
- Invest in Multi-constellation;
- Portugal adopting GALILEO as a EU PNT strategy;
- Promote an open public debate for PNT strategies;
- Classic methods training for positioning, navigation and timing (ex: Celestial Navigation);
- Use of more robust DGPS Stations;
- Invest in e-LORAN;
- Adopt alternative PNT systems;
- Adopt national alternatives with coastal and harbour coverage;
- Make sure, in the Portuguese Navy, that internal and North Atlantic Treaty Organization (NATO) navigation doctrine is being put to practice;
- Implement Autonomous Navigation System in Warships;
- Create an integrated national PNT system with several unclassified systems for civil and military use;
- Use multi-frequency systems (less vulnerable to jamming);
- Use independent PNT systems for redundancy;
- Create systems with flexible architectures that are able to detect failures or flaws and quickly mitigate them (Model adaptation, failure and exception handling as key-aspects of a resilient system, stated in Chapter One).

For these alternatives to be implemented or for the development of a new integrated national PNT system, there needs to be a resilience monitoring plan to identify which failures lead to the complete loss of the system and which ones the system is able to recover from. If the system is available after irregularities occur, it means it is flexible.

All the interviewees, whether they use GNSS for positioning, navigation or timing means, considered that their dependency is high (some even depend exclusively on it), in order to achieve their daily work objectives. On the other hand, they all consider that it is possible to keep going on if the GNSS they use are unavailable. It will, simply, take longer than usual and some concepts must be revised such as: Classic Topography or Celestial navigation. “We should invest more in Celestial Navigation and practice it more, it is useful knowledge and should not be forgotten”[226].

Some stakeholders confessed that they are not specifically prepared in case of GNSS failure and that the population is not able to reach an unknown destination without GPS anymore as it is used for almost everything. Nevertheless, they acknowledge the vulnerability and do not neglect classic methods training as an, always available, alternative.

Some systems operated aboard Portuguese Warships depend, exclusively, on GPS information and have the capability to send out an alarm in case of a GPS unavailability period. If they are not available, the information superiority that the Portuguese Navy is supposed to have to compile the actual maritime picture, will be severely compromised.

The National Network for military and civil use (for organisations that require high precision and accuracy services), SERVIR (provided by the Portuguese Army), is not available if there is no GPS signal. Also, the national service for maritime pollution assistance (Serviço de Combate à Poluição no Mar) also uses GNSS in case of maritime pollution incidents.

Currently, the problem is not solely the GPS dependency: “We are not so dependent on GPS anymore but we are dependent on GNSS.[227]”

The Portuguese PNT Stakeholders already have several GNSS (more specifically GPS) alternatives in use or in development (in partnership with other countries):

- Radar Navigation – necessary to always know the constraints that it implies to the levels below (Constraints)[228];

[226]Translated by the Author.

[227]Translated by the Author.

[228]Nancy Leveson, pp 12-13.

- GALILEO, as a civil GNSS, will be less vulnerable in case of political or military conflicts - there needs to be communication between the different levels of control for effectiveness (Levels of control) as described in Chapter 3[229];
- GALILEO's Public Regulated Service (similar to the Military GPS service) is less vulnerable to jamming and spoofing (larger frequency spectrum) - a relationship between the different variables is required for the actual state to correspond to the process model (Process models)[230];
- With the completion of GALILEO's satellites constellation, there will be total global coverage and interoperability between GALILEO and other constellations - improving the signal in urban canyons;
- The fact that GALILEO will help Search and Rescue through a connection with COSPASSARSAT – a relationship between the different variables is required for the actual state to correspond to the process model (Process models);
- GALILEO will have four atomic clocks (greater time reference accuracy);
- Multi-constellation (when all GNSS have fully operational capability) is expected to make it possible to know on which side of the road a destination is - there needs to be communication between the different levels of control for effectiveness (Levels of Control);
- The use of RTK as an alternative - a relationship between the different variables is required for the actual state to correspond to the process model (Process models);
- The use and training of traditional methods (Celestial navigation, classic topography and hydrography) - necessary to always know the constraints that it implies to the levels below (Constraints);
- The use of Visual Landmarks navigation and Dead Reckoning("Determination without the aid of celestial navigation of the position of a ship from the

[229]Nancy Leveson, pp 12-13.
[230]*Ibidem.*

record of the courses sailed, the distance made, the known starting point and the known estimated drift")[231] - necessary to always know the constraints that it implies to the levels below (Constraints);

- The use of marine paper navigation charts in order to keep the position updated - there needs to be communication between the different levels of control for effectiveness (Levels of Control);
- The use of the National Geodetic Control Network - a relationship between the different variables is required for the actual state to correspond to the process model (Process models);
- The use of Marine Inertial Navigation Systems - there needs to be communication between the different levels of control for effectiveness (Levels of Control);
- The use of the Doppler Radar Systems - there needs to be communication between the different levels of control for effectiveness (Levels of Control);
- The use of GGPS (Geodetic GPS) for hydrographic means - there needs to be communication between the different levels of control for effectiveness (Levels of Control).

5.2 Portuguese PNT actual picture

Based on the Online Questionnaire and the Personal Interviews, an actual Portugal PNT picture was created and can be seen on Figure 23. The solutions and alternatives that have not even started developing (some may never be developed as they are personal opinions of the interviewees) are represented in red. The solutions represented in orange are in development but still in a precarious state. The alternatives and solutions represented in yellow are in development but still not close to being fully developed. In green, are the solutions or alternatives that are already being used or ready to be used.

[231]Britannica, *Dead Reckoning*, https://www.britannica.com/technology/dead-reckoning-navigation, (accessed July 2017).

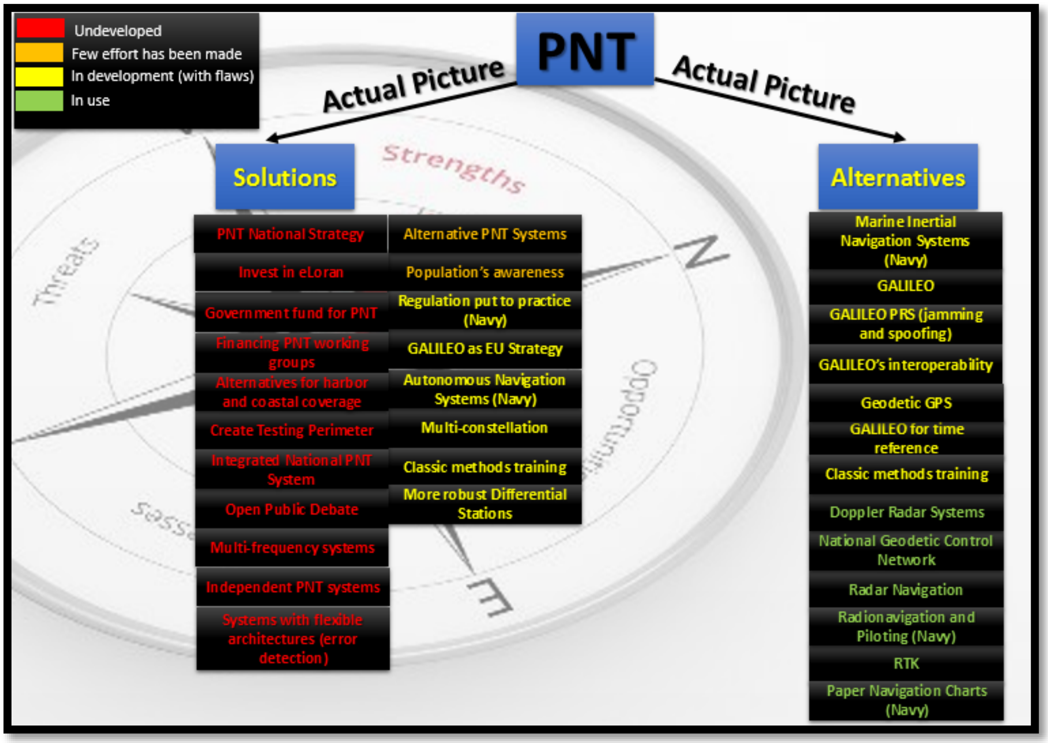


Figure 23 - Portuguese Actual PNT Picture

Analysing, both, the Online Questionnaire data and the Personal Interview data, it can be seen that most PNT Stakeholders believe that something should be done about Portugal's dependency on Europe, Russia, United States of America and China for PNT information. Nevertheless, most also recognize that in the actual financial and social Portuguese picture, it is not advantageous to invest in regional alternatives or developing our own PNT systems. Firstly, there is a common perception of low probability of, in the nearest future, losing both NATO and EU alliances – which means Portugal will be able to advance in accordance with the EU and NATO allies. Secondly, it is assumed that it is very unlikely that all systems should fail at the same time and, thirdly, most of the stakeholders stated that they have alternatives. These alternatives may be robust PNT systems or simple classic methods for obtaining PNT information.

By analysing the Personal Interviews, it was possible to conclude that the concepts that emerged from the interviews all relate to each other, according to Leveson's advices presented in Chapter 3 – Definition of the task; data collection; <u>construction of the</u>

hierarchical control structure; bad control analysis; and review and analysis of accidents[232]:

- GNSS dependency leads to Vulnerability;
- In order to mitigate this vulnerability there are alternative PNT methods that can be used and overall future solutions that can be adopted;
- These solutions also include improving GNSS characteristics in order to have more robust systems;
- They solutions are also important for having system redundancy;
- Alternative solutions and redundancies have inherent costs;
- When considering the costs, there are two possible ways to look at this issue: through a resilient economic way or an efficient economic way.

5.3 Jamming Trial

The three jamming trials performed in this study were performed over a period of 72 hours, aboard a Portuguese warship. Two hand-held jammers were used: J242-G and J220-B, already been used during the SENTINEL Project. The J242-G, according to the manufacturer, has an output power of 2.0W and a shielding radius of 15 metres. The J220-B model has an output power of 0.4W and a shielding radius of 8 metres. Other specifications are presented in APPENDIX H. There are not any further detailed technical specifications due to the language barrier between the Author and the Seller, which failed to give out further details on the jammers.

To assess the jammers impact on the GPS normal functioning, National Marine Electronics Association (NMEA) data (Standard data format supported by all GPS manufacturers[233]) was directly transferred to a portable computer using a free open source program named Putty[234] with a R232 cable, during normal operations and jamming

[232]Nancy Leveson, pp 25-30.

[233]Erik Gakstatter, *What Exactly Is GPS NMEA Data?*, GPS WORLD, 2015, http://gpsworld.com/what-exactly-is-gps-nmea-data/, (accessed June 2017).

[234]http://www.putty.org/

periods. After parsing the NMEA data, it was computed in order to find out the variation between each latitude and longitude coordinates and, also, speed values, leading to the graphs previously presented in Chapter 4. In the raw data, before it was computed, during the jamming periods the positioning data – latitude and longitude – was null which means, after it was processed it was possible to see – graphically - the effective jamming periods.

The data extraction was made directly to the computer through the open source FSH View Software[235]. This led to surprising facts as the jammer that was thought to be more powerful, the J242-G model with a total output power of 2.0W, turned out to be the least effective. The J220-B model was the most effective (and cheapest) model used. When turned on, instantly all the GPS dependent systems tended to fail – with a radius of 30 metres. The normal GPS signal is very weak by itself, due to the satellite-receiver distance, so these values were only possible because of the jammers. This can be proved comparing the "no-jamming" periods with the jamming periods screenshots, previously presented in Chapter 4.

Figure 24 - R&S FSH3 Spectrum Analyzer

In all the three trials, different distances to the GPS antenna were used for each jammer: 1m, 10m, 30m and 50m approximately.

When the J220-B model was operating, alarms sounded on the bridge making the environment more hostile and stressful. Nevertheless, the surprise factor is very

[235]https://www.rohde-schwarz.com/software/fsh/

important and, in this case, it was not possible to test the crew's readiness when submitted to a GPS-denied environment, as they knew that these specific tests were being conducted. The environment, though, was still stressful leading crew members to interrogate when the tests would be over. No emergency/solving procedures were found or used and no technical services were informed. These results and alarms going off were already partially expected according to GLA's previous Jamming Trials.

Firstly, most warships operate basic GPS systems, using the C/A-code. These are vulnerable to jamming when this is not any other physical equipment that can complement this GPS information loss – which was the case. Secondly, navigation doctrine that is still being taught and used, is being put to side due to the users trust on GPS for PNT information. Users know, for a fact, that GPS might not be available but it seems to be available every day, leading to overreliance and a disregard of more detailed and complex procedures. Thirdly, there are not any implemented routines of checking if the GPS and GPS-dependent systems are in normal functionality. Users presume that the position is correct if there is not any alarm. The fact is, that during the GPS trials, if the jamming signal was not powerful enough (when there was a greater distance from the jammer to the GPS antenna), the Radar, ECDIS and GPS did not black out, they simply kept showing an out of date position that the users do not know if it is trustworthy or not, but still keep using it as positioning reference.

At last, in case of a jamming event, no internal Standard Operational Procedures (SOP) was found aboard and there are not any anti-jamming antennas or filters to mitigate these kinds of events.

On the jamming trials results, the first and third trials were not as reliable as the first trial due to the fact that the naval unit was anchoring in harbour.

On Table 6, the impact of both jammers can be seen according to the measured distances (Green – Systems working normally; Yellow – Positioning errors but no alarms; Red – Alarms and no PNT information).

Distance(m)	MODEL J242-G 	MODEL J220-B 
1		
10		
30		
50		

Table 6 - Jammers impact (1,10,30,50m)

On Figure 25, a vulnerability assessment is made due to the crew's behavior and implemented routines.

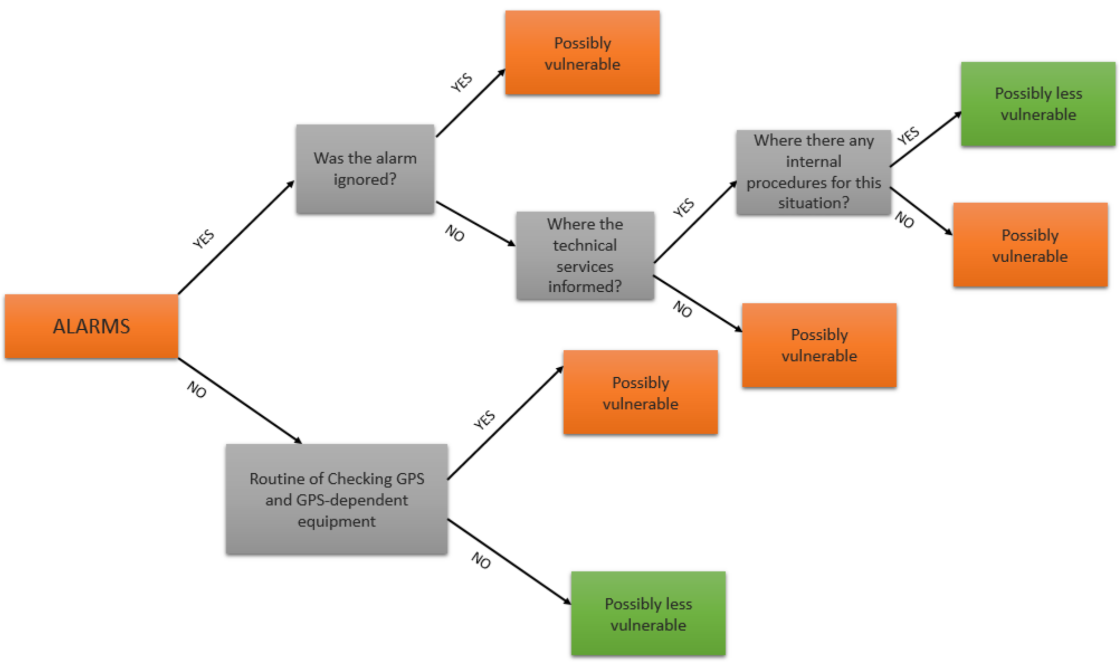


Figure 25 - Vulnerability assessment

Observing Figure 25, one may easily conclude that if there are not implemented routines for checking the GPS and GPS information dependent systems; if an alarm goes off and the technical services are not aware; or if there are not any internal procedures implemented for this specific case: a Warship is possibly vulnerable when submitted to a GPS-denied environment.

The main question of the Project, “Why should PNT Systems be resilient?” was responded throughout the Project Report. PNT Systems should be resilient in order to predict, avoid and mitigate possible accidents. HRO, like the Portuguese Navy, depend on continuous PNT information for maintaining information superiority and to be able to operate in calamitous scenarios. This means that the PNT systems they operate, per example, in Warships, should:

- Send out warnings when in a degraded condition;
- Have flexible architectures;
- Be able to quickly recover when submitted to hazardous conditions;
- Have redundancies;
- Operators should have routines for a proper system’s-health assessment and procedures in case there is equipment failure.

This is only possible if there other PNT alternatives do not exist aboard, apart from the GPS, whose vulnerabilities have been referred throughout the report.

According to the secondary questions: “How can a PNT System be resilient?” Briefly, a PNT System is resilient if:

- It serves all types of navigation (Restricted Waters Navigation, Coastal Navigation and Open Sea Navigation);
- It is compatible with augmentation systems;
- Allows unlimited users;
- Operates with geodetic and time reference systems;
- It informs the users if degradation occurs;
- It is compatible with shipborne equipment;
- It is accurate; precise; available; reliable; continuous; has integrity monitoring and know its integrity risk.

“What are the Portuguese PNT Stakeholders looking for in a PNT System?” The Portuguese PNT Stakeholders are mainly looking at the following performance requirements in the following order:

- Availability;
- Continuity;
- Precision;
- Accuracy;
- Coverage;
- Integrity.

Also, they believe that the best possible alternatives to GNSS would be the creation of Local Systems – Pseudolites was presented as an example for these systems in the questionnaire - and Traditional Navigation Training (ex: Celestial Navigation). Most of them depend on PNT systems for Positioning, Navigation and Timing in the previous order.

"What is the current perspective of PNT Systems in Portugal?" Currently Portugal:

- Is taking part, with the EU, in the GALILEO Project;
- Has Differential GPS in use and operational;
- Has Doppler Radar Systems in Aircrafts;
- Has a National Geodetic Network in currently available;
- Radar Navigation and Visual Landmarks are possible independent to PNT alternatives;
- Real-Time Kinematics are currently being used;
- Classic Navigation Methods are still being taught in Military Academies and Universities.

However, Stakeholders believe that we should invest in e-LORAN; have a Government fund for PNT; finance PNT working groups; create alternatives for harbour and coastal coverage; implement multi-frequency systems and create a National Test Perimeter for assessing system vulnerability.

"Are the Portuguese Warships vulnerable to (un)intentional GPS information denial?" Most Portuguese Warships' GPS systems operate the SPS with the normal C/A-code. Only few of them operate the P(Y)-Code. This means, they are not immune to (un)intentional jamming and, only few, are partially protected from Spoofing through the P(Y)-code. Apart from this:

- There are no internal procedures for assessing the GPS System's health periodically;
- There aren't any anti-jamming antennas or filters;
- There aren't also procedures in case there is GPS unavailability;
- There are no training programs for this matter in the Portuguese Navy's internal training plan.

It is highly recommended, in a near future, to integrate other PNT Systems with our traditional outdated GPS System, like Inertial Navigation Systems, and make a national assessment on how anti-jamming antennas should be implemented and how they should be positioned.

Chapter 6 – A path for a resilient PNT System in Portugal

Firstly, in order to create a national resilient PNT system, it is important to think back on what characteristics make a system resilient. As referred before, a resilient system should have the capacity to:

- Handle its own failures;
- Manage exceptional events;
- Adapt according to the business and organisational environment;
- Handle changes that were not predicted when the models were designed;
- React in case "cascading" events occur[236];
- Have the capacity to absorb disruptions without having a breakdown;
- Be flexible and respond to external changes;
- Have a considerable margin to the performance boundaries;
- Be tolerant and have healthy interactions between the scales above and below.[237]

Most of the Stakeholders interviewed in this project have back-up systems in case the PNT systems they use, fail. Nevertheless, one the factors that, most of them, considered vital for responding to their daily service needs was Availability. This is not, always, possible when the only PNT System they operate is a GNSS, due to several intentional or unintentional factors that have been referred before. Throughout this project, also, the vulnerability of a Portuguese Warship was tested, when submitted to GPS-denied environment and, the results, were not positive. There were not any redundant systems, pre-planned responses or routines for responding to these matters.

According to the theoretical approach initially made, the Questionnaire and Interview results and the GPS Jamming Trials, the following advices can be considered individual steps for creating a path to a Portuguese Resilient PNT System:

[236]Pedro Antunes, Hernâni Mourão, pp 7-9.

[237]Erik Hollnagel, David Woods, Nancy Leveson, p 23.

1. Population and Government Awareness – explain GNSS' possible vulnerabilities and show other countries' progress on PNT alternatives;
2. Promote a Public Debate – PNT Stakeholders should discuss Portugal's PNT future and possible solutions;
3. Create a National Budget on PNT;
4. Designate a National PNT Authority – the Portuguese Government should designate a new PNT Cabinet for projects approval and coordination;
5. Promote PNT investigation groups – for investigating and developing resilient alternatives;
6. Create a National Test Perimeter – to submit projects to adverse conditions;
7. Invest in National Industry - or lead agreements with international industries for manufacturing;
8. System Tests – is it independent? Does it work in critical situations? Does it have a flexible architecture? Does it recover from unpredicted events?
9. Implementation Plan – according to Portugal's economic situation, the stakeholders should be the ones to invest in new equipment for operating with a new PNT System (it is not utopic if they are shown the advantages of moving forward);
10. Keep participating and bringing new alternatives to international projects to create funds for project support;
11. Integrate our new resilient PNT System with other systems - for redundancy, global coverage, permanent availability, greater precision and accuracy and reliability;
12. Periodic collection and analysis of Stakeholder's feedback;
13. Periodic National Conferences - for development and upgrades;

A visual representation of these measures can be seen on APPENDIX J.

This process is expected to a take long time until it is fully implemented as it requires funds, complex engineering and an urge to develop and enrich the Portuguese participation in the PNT Industry.

However, there are several actions that can be implemented in a short period of time, especially in the Portuguese Navy (which was studied in greater detail during this project) such as:

- Implementing existing doctrine for Piloting and Navigating in Coastal waters;
- Creating SOPs for responding in a hazardous environment (per example, when submitted to Jamming or Spoofing);
- Include these procedures in the National Basic Training Plan for Warships;
- Create internal technical procedures for improving the resilience of the equipment receiving the GNSS signals (according to the U.S. Department of Homeland Security' report[238]). No internal procedures were found for this matter, during the research made in this project.

[238]United States Department of Homeland Security, pp 5-6.

Conclusion

In the development of this project, the concepts that were necessary for understanding the definition of Resilience and PNT Systems were studied. Using this theoretical approach, doing questionnaires, personal interviews and a Jamming Trial, made it possible to conclude what is the actual Portuguese PNT Picture; which is the path for developing our own resilient PNT System; and to understand how vulnerable the Portuguese Warships when submitted to a jamming attempt.

High Reliability Organisations need to have their main services guaranteed in critical situations. This means they must operate resilient systems for being able to assume control and have information superiority in catastrophic scenarios. The Portuguese Navy is one of these HRO that is several times submitted to operate in hazardous conditions, where positioning, navigation and timing data is crucial for mission accomplishment. However, if the actual PNT Systems aboard the Portuguese Navy Warships are not upgraded, they will always be vulnerable to intentional GPS-denial events, like jamming or spoofing. The same situation applies to all the Organisations and National Services that depend, only or mainly, on GPS.

The methodology for analysing the Questionnaires and Interviews was quite complex as some parameters could not be compared. The organisations or individuals that were interviewed, belonging to a Stakeholder group, were not totally representative of that group, making the data unable to be totally conclusive. In order to perform a valid analysis, more representative elements of each stakeholder group should have been interviewed, which would require a greater time period for this part of the study.

The methodology used for assessing the Portuguese Navy's vulnerability helped realizing that prevailing internal and NATO doctrine should be enforced and, procedures and pre-planned responses for vulnerable conditions, should be implemented and trained.

The methodology used for the Questionnaires and Interviews to the Stakeholders helped to realize how vulnerable Stakeholders consider themselves by operating GNSS and if they have systems or procedures as alternatives or back-ups, in case of GNSS unavailability. Moreover, it was possible to create the actual Portuguese PNT picture based on the Stakeholders opinions and create a path to develop a resilient Portuguese PNT System.

Overall, the initial objectives were accomplished. Nevertheless, some particularities could be improved such as the possibility of performing more Jamming Trials in different Naval Units in order to assess if the conclusions would be similar; have a more equal representation of each group of stakeholders for better data analysis; and do further analysis on the Spectrum Analyzer data for more detailed and technical conclusions.

There were several constraints during the project, especially the theoretical approach that had to be performed before and after the jamming trials. Before the jamming trial it was necessary to define procedures and understand which systems depended on GPS information, to enable the data extraction. After the Jamming Trial, the same process had to be repeated for executing the NMEA data analysis. Also, getting in touch with the Stakeholders was not trivial. Firstly, because of the short period of time available for this matter and, secondly, because some organisations and individuals never replied to the questionnaire and interview request.

As a final suggestion for future projects: It is recommended to perform a study on the GPS antenna installation aboard Portuguese Navy Warships and the creation of internal doctrine for this matter, with the intent to reduce vulnerability, make the receivers more resilient – per example installing Radiofrequency filters or CRPA – and implement new resilient PNT alternatives.

Bibliography

ALTHOS, *GPS ROVER STATION*, http://www.wirelessdictionary.com/wireless_dictionary_GPS_Rover_Station_Definition.html, (accessed January 2017).

ANTUNES, Pedro, MOURÃO, Hernâni, *Resilient Business Process Management; Frameworks and Services*, Lisbon, Faculty of Sciences of the University of Lisbon, 2011.

BRITANNICA, *Dead Reckoning*, https://www.britannica.com/technology/dead-reckoning-navigation, (accessed July 2017).

BAILEY, Kathryn, *Moving Celestial To Terrestrial: Leveraging Pseudolites For Assured PNT*, http://www.cerdec.army.mil/news_and_media/Moving_celestial_to_terrestrial_leveraging_pseudolites_for_Assured_PNT/, (accessed December 2016).

BIDIKAR, Bharati*, et. al*., "Satellite Clock Error and Orbital Solution Error Estimation for Precise Navigation Applications", Scientific Research, 2013.

BUCKLEY, Paul, "Next-gen inertial sensors aim to replace GPS", *Smart2zero*, 2016, http://www.smart2zero.com/news/next-gen-inertial-sensors-aim-replace-gps, (accessed July 2017).

BUESNEL, Guy, et al., "Make it real: Developing a test framework for PNT systems and devices", GPS WORLD, 2016, http://gpsworld.com/make-it-real-developing-a-test-framework-for-pnt-systems-and-devices/, (accessed January 2017).

CAMERON, Alan, "Resilient", GPS WORLD, January Issue, 2016.

———, "A long look at advanced Multisensor Navigation and Positioning", *GPS WORLD*, 2014, http://gpsworld.com/a-long-look-at-advanced-multisensor-navigation-and-positioning/, (accessed July 2017).

———, "Double trouble: GNSS over-reliance and its costs", GPS WORLD, 2017, http://gpsworld.com/double-trouble-gnss-over-reliance-and-its costs/?utm_source=gnss_dt&utm_medium=email&utm_campaign=gnss_dt_06282017&eid=376815012&bid=1799490, (accessed July 2017).

CARMO, Hermano, FERREIRA, Manuela Malheiro, *Metodologia da Investigação, Guia da Auto-aprendizagem*, 2ª Edição, Lisboa, Universidade Aberta, 2008.

CIVIL ENGG DICTIONARY, *Sources of errors in GPS*, http://www.aboutcivil.org/sources-of-errors-in-gps.html, (accessed July 2017).

COFFED, Jeff, *The Threat of GPS Jamming, The Risk to an Information Utility*, Exelis, New York, 2014.

CURRY, Charles, *Delivering a National Timescale using e-LORAN*, Chronos Technology, Lydbrook, 2014.

————, *Sentinel Project Report on GNSS Vulnerabilities*, 2014.

————, *GPS-Free UTC TimeScale Using e-Loran*, International Timing and Sync Forum 2015, Edinburgh, 2015.

————, *Latest Update on GPS Jamming & Susceptibility Trials*, 2015, http://www.chronos.co.uk/files/pdfs/pres/2015/ITSF/ITSF_LatestUpdateonGPSJamming&SusceptibilityTrials-Curry.pdf, (accessed January 2017).

DEMPSTER, Andrew, *Boaters beware GPS vulnerable to interference and jamming*, 2016, http://www.marinebusinessworld.com/n/Boaters-beware-GPS-vulnerable-to-interference-and-jamming/81275?source=google.pt, (accessed April 2017).

DICK, Steven J., LAUNIUS, Roger D., *Social Impact of Spaceflight*, NASA History Division, Washington DC, 2007.

DIVIS, Dee Ann, "Proposal for U.S. eLoran Service Gains Ground", 2014, http://www.insidegnss.com/node/3853, (accessed October 2016).

EUROPEAN SPACE AGENCY, *GALILEO clock anomalies under investigation*, 2017, http://www.esa.int/Our_Activities/Navigation/Galileo_clock_anomalies_under_investigation, (accessed May 2017).

EUROPEN SPACE AGENCY NAVIPEDIA, *GALILEO Performances*, 2011, http://www.navipedia.net/index.php/Galileo_Performances, (accessed June 2017).

————, *GPS Performances*, 2011, http://www.navipedia.net/index.php/GPS_Performances, (accessed June 2017).

————, *GPS Services*, 2011 http://www.navipedia.net/index.php/GPS_Services, (accessed June 2017).

————, *GPS Signal Plan*, 2011, http://www.navipedia.net/index.php/GPS_Signal_Plan, (accessed June 2017).

————, *SBAS Fundamentals*, http://www.navipedia.net/index.php/SBAS_Fundamentals, (accessed January 2017).

————, *Wide Area RTK (WARTK)*, http://www.navipedia.net/index.php/Wide_Area_RTK_(WARTK), (accessed January 2017).

FEDERAL AVIATION ADMINISTRATION, *The Global Loran/eLoran Infrastructure Evolution, A Robust and Resilient PNT Backup for GNSS*, USA, 2014.

———, *Satellite Navigation – GBAS – How it works*, https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/laas/howitworks/, (accessed March 2017).

FISHERIES AND OCEANS CANADA COAST GUARD, *Primer or GPS and DGPS*, Canadian Coast Guard, 2000.

FUTAKI, Károly, Danube Flood risk Project, *Stakeholder Selection Strategy*, VKKI, Budapest, 2010.

GAKSTATTER, Eric, "What Exactly Is GPS NMEA Data?" *GPS WORLD*, 2015, http://gpsworld.com/what-exactly-is-gps-nmea-data/, (accessed June 2017).

GENERAL LIGHTHOUSE AUTHORITIES OF THE UNITED KINGDOM AND IRELAND, *GPS Jamming Trial*, Executive Summary Report for Website, United Kingdom, 2008.

———, "Briefing note: Evolution from Loran-C to eLoran", issue 1.0, 2010.

GOHUB, "In 2017, GPS Spoofing is the real bane of Pokémon GO", 2017, https://pokemongohub.net/2017-gps-spoofing-real-bane-pokemon-go/, (accessed May 2017).

GPS GOV, *Information About GPS Jamming*, http://www.gps.gov/spectrum/jamming/, (accessed January 2017).

———, *Wide Area Augmentation System (WAAS) Status and History*, 2014, http://www.gps.gov/multimedia/presentations/2014/09/ION/bunce.pdf, (accessed December 2016).

GPS WORLD, "Anti-jam Protection by Antenna", 2013, http://gpsworld.com/anti-jam-protection-by-antenna/, (accessed June 2017).

———, "Iridium launches alternative GPS PNT service", GPS WORLD, 2016, http://gpsworld.com/iridium-launches-alternative-gps-pnt-service/, (accessed January 2017).

———, "HRL Labs to develop inertial sensor tech for DARPA", GPS WORLD, 2017, http://gpsworld.com/hrl-labs-to-develop-inertial-sensor-tech-for-darpa/, (accessed January 2017).

GRANT, Alan, et al., *Understanding GNSS availability and how it impacts maritime safety*, San Diego, The General Authorities of the United Kingdom and Ireland, 2011.

———, WILLIAMS, Paul, BASKER, Sally, "GPS Jamming and its impact on maritime safety", Port Technology International, 2010.

GREJNER-BRZEZINSKA, et al., "Multisensor Navigation Systems: A Remedy for GNSS Vulnerabilities?", Proceedings of the Institute of Electric and Electronics Engineers, Vol. 104 nº 6, June 2016.

HOLLNAGEL, Erik, WOODS, David D., LEVESON, Nancy, *Resilience Engineering, Concepts and Precepts*, Aldershot, Ashgate Publishing Limited, 2006.

HOW GPS WORKS, http://www.how-gps-works.com/glossary/ephemeris-error.shtml, (accessed July 2017).

HU, Qing, *Development of an Automatic Identification System Autonomous Positioning System*, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4701297/, (accessed March 2017).

INNOVATE UK, THE UK SPACE AGENCY, THE ROYAL INSTITUTE OF NAVIGATION, *Economic Impact of a disruption to GNSS*, Showcase Report, London, London Economics, 2017.

INTERNATIONAL LORAN ORGANIZATION, *Enhanced Loran (eLoran)*, Definition Document, 2007.

INTEGRATED MAPPING LTD., *How GPS Works*, https://www.maptoaster.com/maptoaster-topo-nz/articles/how-gps-works/how-gps-works.html, (accessed May 2017).

INTERNATIONAL MARITIME ORGANIZATION, *Resolution A.915 (22), Revised Maritime Policy and Requirements for a Global Navigation Satellite System*, IMO, 2001.

———, Subcommittee on the Safety of Navigation, *Report to the Maritime Safety Committee*, IMO, 2011, p 18.

JAN, Shau-Shiun, TAO, An-Lin, *Comprehensive Comparisons of Satellite Data, Signals, and Measurements between the BeiDou Navigation Satellite System and the Global Positioning System*, National Cheng Kung University, Taiwan, 2016.

JAPAN TIMES, “South Korea revives GPS backup project after alleged jamming by North Korea”, 2016, http://www.japantimes.co.jp/news/2016/05/02/asia-pacific/south-korea-revives-gps-backup-project-after-alleged-jamming-by-north-korea/#.WAVG1eArLIV, (accessed October 2016).

JOHN A. VOLPE NATIONAL TRANSPORTATION SYSTEMS, *Vulnerability Assessment of the Transportation Infrastructure relying on the Global Positioning System*, Final Report, Massachusetts, 2001.

KINTNER, Paul, HUMPHREYS, Todd, HINKS, Joanna, “GNSS and Ionospheric Scintillation”, Inside GNSS, July/August Issue, 2009, pp 22-29.

LANGLEY, Richard B., “Innovation: GNSS and the Ionosphere”, GPS WORLD, 2011, http://gpsworld.com/innovation-gnss-and-ionosphere-11036/, (accessed May 2017).

LAST, David, “U.S. Nears eLoran Decision with Broad International Implications”, Washington View – Inside GNSS, March/April Issue, 2015, pp 24-31.

LEVESON, Nancy, *A New Accident Model for Engineering Safer Systems*, Massachusetts Institute of Technology, Massachusetts, 2004.

LO, Sherman, “Alternative PNT: Assured Service, GNSS Backup”, Inside GNSS, September/October Issue, 2015, pp 32-33.

MADRY, Scott, *Global Navigation Satellite Systems and their Applications*, New York, Springer Science + Business Media LCC, 2015.

MCMURDO, *Resilient PNT, At the Core of Mission Critical Applications*, http://www.mcmurdogroup.com/company/orolia-group/what-is-resilient-pnt/, (accessed May 2017).

MCNEFF, Jules, “Changing the Game Changer”, “The Way Ahead for Military PNT”, Inside GNSS, November/December Issue, 2010, pp 47-48.

MONTEIRO, Luís, *Designing, configuring and validating the Portuguese DGPS Network*, PhD Thesis through Nottingham University, Nottingham, 2004.

NATIONAL AIR AND SPACE MUSEUM SMITHSONIAN INSTITUTE, *PNT (Positioning, Navigation and Timing)*, 2012, https://timeandnavigation.si.edu/multimedia-asset/pnt-positioning-navigation-and-timing, (accessed March 2017).

NATIONAL SECURITY PRESIDENCIAL DIRECTIVES, *NSPD-39: U.S. Space-Based Position, Navigation*, and Timing Policy, 2004.

NEMETH, Christopher P., HOLLNAGEL, Erik, *Becoming Resilient, Resilience Engineering in Practice Volume 2*, Ashgate Publishing Limited, Farnham, 2014.

NORTH ATLANTIC TREATY ORGANIZATION, *Testing direction finder at GPS Jamming Trials*, https://www.ncia.nato.int/NewsRoom/Pages/160905-Sennybridge-GPS-Jamming-Trials.aspx, (accessed January 2017).

NOVATEL, *Real-Time Kinematic*, http://www.novatel.com/an-introduction-to-gnss/chapter-5-resolving-errors/real-time-kinematic-rtk/, (accessed January 2017).

———, *Understanding the Difference Between Anti-Spoofing and Anti-Jamming*, 2013, http://www.novatel.com/tech-talk/velocity/velocity-2013/understanding-the-difference-between-anti-spoofing-and-anti-jamming/, (accessed January 2017).

NTP FAQ, *What is NTP?*, http://www.ntp.org/ntpfaq/NTP-s-def.htm#AEN1259, (accessed March 2017).

O’DRISCOLL, Cillian, BORIO, Daniele, FORTUNY, Joaquim, *Scoping Study on Pseudolites*, European Commission Joint Research Center, 2011.

OFFICE OF MANAGEMENT AND BUDGET, *Terminations, Reductions, and Savings, Budget of the U.S. Government*, Washington D.C., 2009.

———, *Budget of the U.S. Government: Fiscal Year 2010*, U.S.A, 2010.

PACE, Scott, et al., *The Global Positioning System: Assessing National Policies*, California, RAND Corporation, 1995.

PSIAKI, Mark, HUMPHREYS, Todd, *Protecting GPS From Spoofers Is Critical to the Future of Navigation*, http://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation, (accessed January 2017).

RABINOWITZ, Phil, *Section 8. Identifying and Analyzing Stakeholders and Their Interests*, http://ctb.ku.edu/en/table-of-contents/participation/encouraging-involvement/identify-stakeholders/main, (accessed June 2017).

RASMUSSEN, Jens, SVEDUNG, Inge, *Proactive Risk Management in a Dynamic Society*, 1st edition, Karlstad, Swedish Rescue Services Agency, 2000, p 5.

REILLON, Vincent, *Briefing GALILEO: Overcoming obstacles*, History of EU Global Navigation Systems, 2017.

ROYAL INSTITUTE OF NAVIGATION, "UK eLoran abandoned", 2016, https://www.rin.org.uk /NewsItem/4433/UK-eLoran-abandoned, (accessed May 2017).

SEPTENTRIO SATELLITE NAVIGATION, *GNSS Interference*, Belgium, 2012.

SHAW, George et al., *Mitigating the effects of GNSS Interference – GLA monitoring and update on eLoran*, General Lighthouse Authorities of the United Kingdom and Ireland, 2011.

SHKEL, Andrei, "The Chip-scale Combinatorial Atomic Navigator", GPS WORLD, August Issue, 2013, pp 8-10.

SKYBRARY, *Distance Measuring Equipment (DME)*, http://www.skybrary.aero/index.php/ Distance_Measuring_Equipment_(DME), (accessed March 2017).

STAKE, Robert E., *A Arte de Investigação com Estudos de Caso*, Tradução de Ana Maria Chaves, Lisboa, Fundação Calouste Gulbenkian, 2007.

STRALEN, Daved, *High Reliability Organizations*, High Reliability Organizing, http://high-reliability.org/High-Reliability-Organizations, (accessed April 2017).

SUB-COMMITTEE ON THE SAFETY OF NAVIGATION, *Development of an E-Navigation Strategy Implementation Plan*, United Kingdom, International Maritime Organization, 2011.

TAMPERE UNIVERSITY OF TECHNOLOGY, *Basic Principles of Inertial Navigation*, http://aerostudents.com/files/avionics/InertialNavigationSystems.pdf, (accessed December 2016).

THE FREE DICTIONARY BY FARLEX, http://www.thefreedictionary.com/cascading, (accessed May 2017).

THE ROYAL ACADEMY OF ENGINEERING, *Global Navigation Space Systems: reliance and vulnerabilities*, London, 2011, p 8.

TRIMBLE, *Trimble GPS Tutorial - Error Correction*, http://www.trimble.com/gps_tutorial/howgps-error2.aspx, (accessed July 2017).

UCHILL, Joe, *Why GPS is more vulnerable than ever*, http://projects.csmonitor.com/gps/, (accessed April 2017.)

UNITED STATES COAST GUARD NAVIGATION CENTER, *Loran-C General Information*, http://www.navcen.uscg.gov/?pageName=loranMain, (accessed October 2016).

UNITED STATES DEPARTMENT OF HOMELAND SECURITY, *Improving the Operation and Development of the GPS Equipment Used by Critical Infrastructure*, United States Department of Homeland Security, 2017.

UNITED STATES NAVAL OBSERVATORY, *Cesium Atoms at Work*, http://tycho.usno.navy.mil/cesium.html, (accessed October 2016).

UTNEWS, "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea", 2013, https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea, (accessed January 2017).

WILLIAMS, Paul, HARGREAVES, Chris, "UK eLoran – Initial Operational Capability at the Port of Dover", Proceedings of the 2013 International Technical Meeting of The Institute of Navigation, California, 2013.

WILLIAMS, Paul, LAST, David, WARD, Nick, *The Deployment of eLoran in the UK*, General Lighthouse Authorities of the United Kingdom and Ireland, Harwich, 2013.

APPENDIX A

Description: The informative leaflet that was e-mailed do every Portuguese PNT Stakeholder.

A RESILIÊNCIA DOS SISTEMAS PNT: O CASO DE PORTUGAL

Exmº/ª Sr.(a),

No âmbito da realização da dissertação de Mestrado para conclusão do Mestrado em Ciências Militares Navais na Escola Naval da Marinha Portuguesa eu, Aspirante a Oficial, Catarina de Sousa Matos Aresta estou a elaborar um estudo subornidado ao tema: "Resiliência dos Sistemas PNT: o caso de Portugal".

Objectivo do Estudo

O estudo, no qual se pede a sua participação, consiste em identificar qual é para si a importância da modernização dos sistemas PNT (Position, Navigation and Timing) em Portugal e qual o impacto no nosso dia-a-dia caso estes falhem. Como é de conhecimento geral, os sistemas de informação, a tecnologia, a defesa militar, o controlo do tempo e a navegação dependem, de um modo geral, do GNSS. Como está o nosso país preparado para a sua eventual perda, temporária ou permanente?

Implementação

A recolha de informação será feita de duas formas: primariamente através de um curto questionário online com perguntas de resposta rápida, "Sim/Não" e outras a que deverá atribuir uma pontuação às diferentes alternativas.Posteriormente, com data a agendar, uma entrevista pessoal de 3 perguntas de resposta aberta, sujeitas a gravação de voz para posterior processamento de dados. A entrevista terá uma duração máxima de 40 minutos. A informação bruta recolhida será tratada como informação confidencial, não será cedida a entidades exteriores ao estudo e a entrevista poderá ser feita em anónimo, pelo que se considerará que foi cedida pela sua organização/departamento/serviço/autoridade.

O seu papel e expetativas

Pede-se a sua colaboração como especialista na área em que trabalha de acordo com os critérios estabelecidos para a entrevista de *Stakeholders* do *GNSS*. As suas respostas e o seu conhecimento serão fulcrais à continuidade do estudo, no entanto, poderá interromper e terminar a entrevista, sem qualquer motivo de justificação. É de elevada importância frisar que nenhuma informação poderá ser utilizada para uma avaliação individual,

É esperado que possa contribuir com o seu conhecimento e experiência na sua área. Este estudo servirá para a construção do panorama atual dos sistemas PNT em Portugal, qual o conhecimento existente nesta área e qual a visão para um futuro próximo.

Responsabilidade e contactos

Responsabilidade: Comandante Victor Plácido da Conceição (placido.conceição@marinha.pt)

Contacto: Aspirante Catarina de Sousa Matos Aresta (catarina.sousa.aresta@marinha.pt) 914272730

Figure 26 - Stakeholder's request for participation

APPENDIX B

Description: The Online Questionnaire, through Google Forms, that was answered by all the interested PNT Stakeholders.

Questionário de apoio a Dissertação de Mestrado subordinada ao tema: "Resiliência dos Sistemas PNT: o caso de Portugal"

Exmº/ª Senhor(a),
Este questionário destina-se, exclusivamente, a contribuir para um estudo para a elaboração de uma Dissertação de Mestrado.
Toda a informação bruta será tratada como Confidencial. Este questionário não serve para o avaliar como indivíduo nem a sua Empresa/Organização.
Pede-se que responda da forma que lhe for pedida.

Muito obrigada!

Email address *

Valid email address

This form is collecting email addresses. Change settings

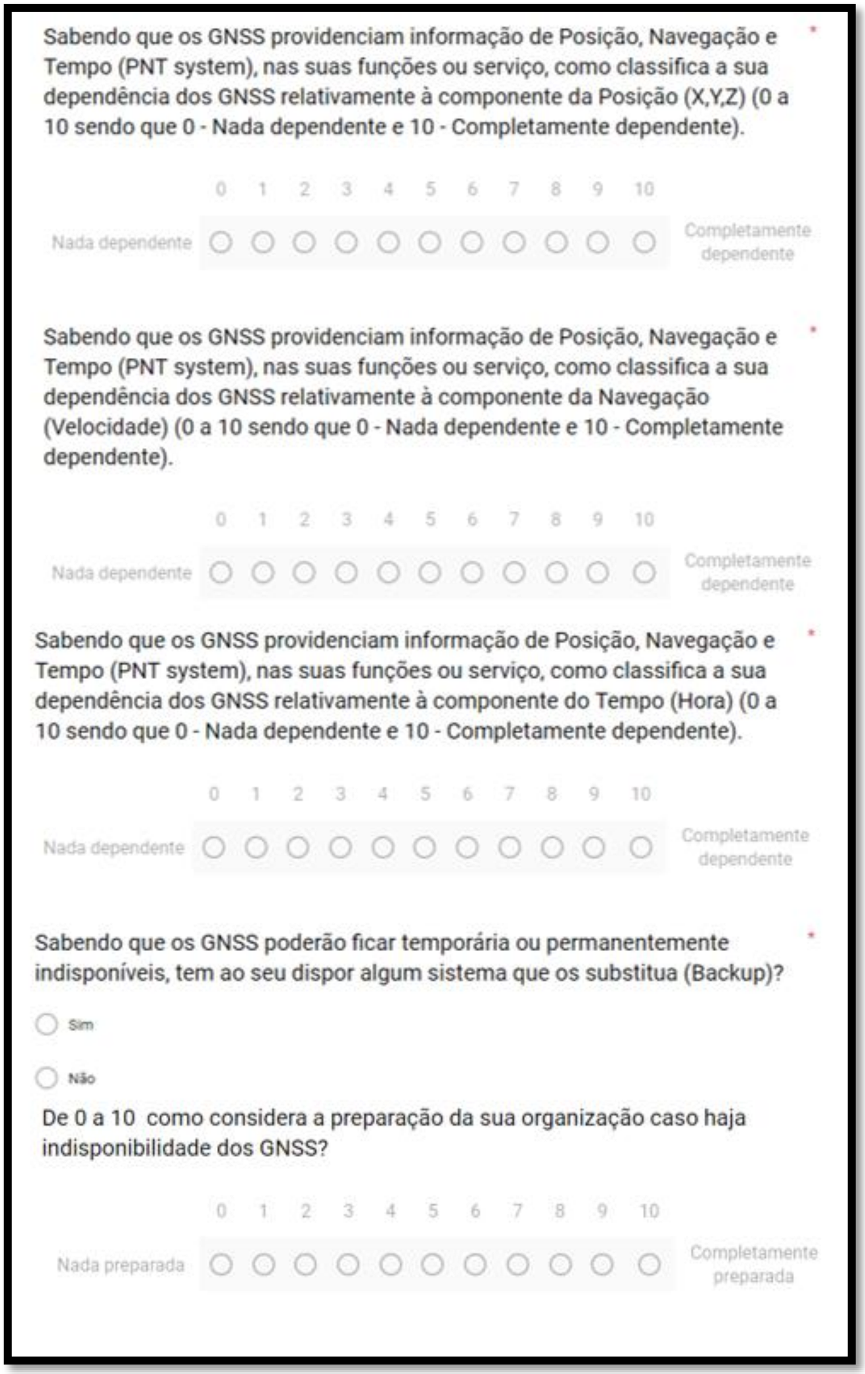
Trabalha/trabalhou com GNSS? Sim/Não (Se negativo salte a próxima questão). *

- Não
- Sim

Se respondeu "Sim" em que grupo(s) se enquadra?

- Investigação
- Autoridade Reguladora
- Autoridade de Controlo e Vigilância
- Ensino
- Utilizador (Condução da navegação)
- Utilizador (Referência de tempo)
- Utilizador (Localização)
- Fornecedor de Serviços GNSS (ex: DGPS)
- Fornecedor de Serviços dependentes de GNSS
- Other...

Figure 27 - Questionnaire (page 1)



Sabendo que os GNSS providenciam informação de Posição, Navegação e Tempo (PNT system), nas suas funções ou serviço, como classifica a sua dependência dos GNSS relativamente à componente da Posição (X,Y,Z) (0 a 10 sendo que 0 - Nada dependente e 10 - Completamente dependente). *

	0	1	2	3	4	5	6	7	8	9	10	
Nada dependente	○	○	○	○	○	○	○	○	○	○	○	Completamente dependente

Sabendo que os GNSS providenciam informação de Posição, Navegação e Tempo (PNT system), nas suas funções ou serviço, como classifica a sua dependência dos GNSS relativamente à componente da Navegação (Velocidade) (0 a 10 sendo que 0 - Nada dependente e 10 - Completamente dependente). *

	0	1	2	3	4	5	6	7	8	9	10	
Nada dependente	○	○	○	○	○	○	○	○	○	○	○	Completamente dependente

Sabendo que os GNSS providenciam informação de Posição, Navegação e Tempo (PNT system), nas suas funções ou serviço, como classifica a sua dependência dos GNSS relativamente à componente do Tempo (Hora) (0 a 10 sendo que 0 - Nada dependente e 10 - Completamente dependente). *

	0	1	2	3	4	5	6	7	8	9	10	
Nada dependente	○	○	○	○	○	○	○	○	○	○	○	Completamente dependente

Sabendo que os GNSS poderão ficar temporária ou permanentemente indisponíveis, tem ao seu dispor algum sistema que os substitua (Backup)? *

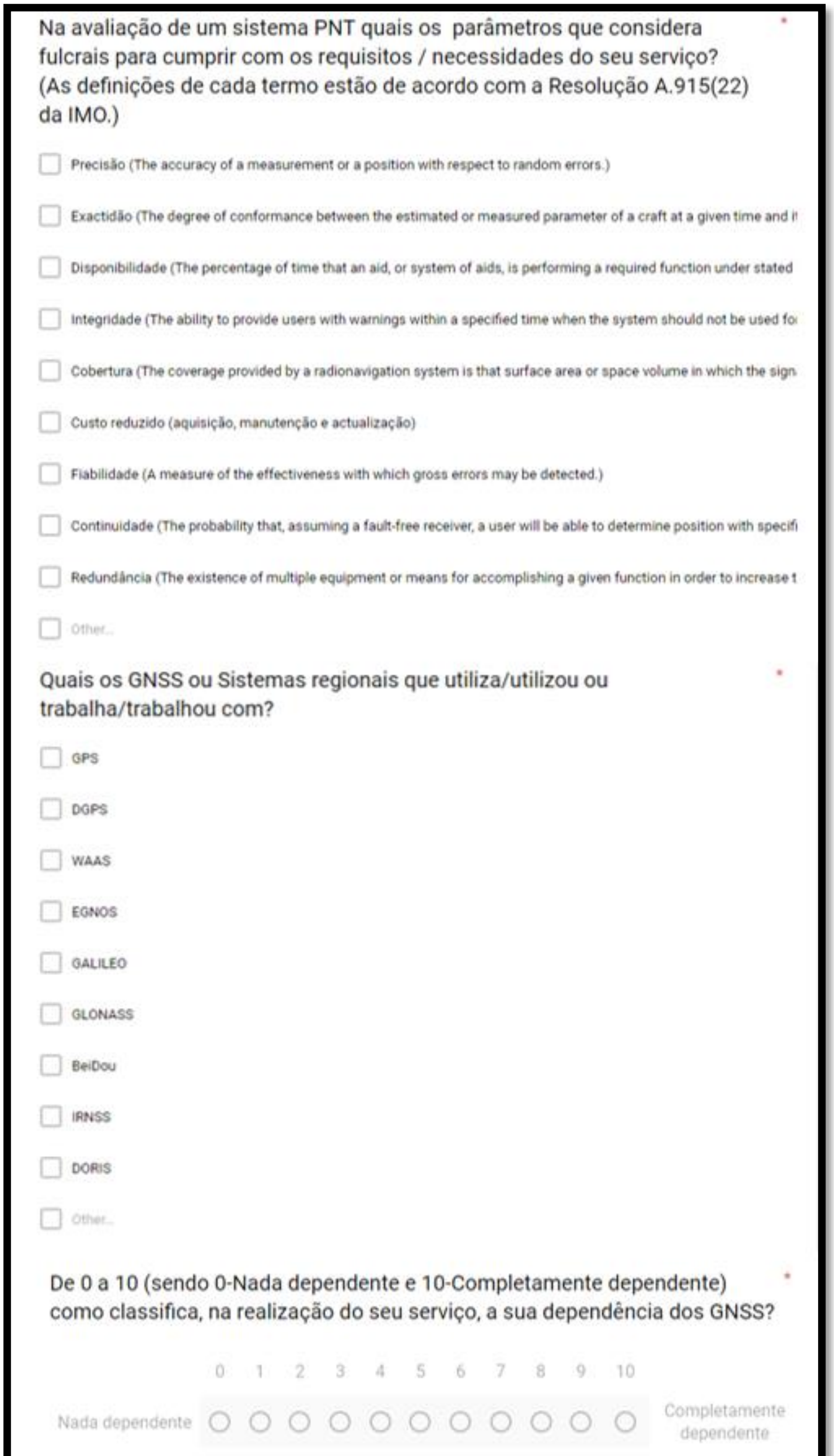
○ Sim

○ Não

De 0 a 10 como considera a preparação da sua organização caso haja indisponibilidade dos GNSS?

	0	1	2	3	4	5	6	7	8	9	10	
Nada preparada	○	○	○	○	○	○	○	○	○	○	○	Completamente preparada

Figure 28 - Questionnaire (page 2)



Na avaliação de um sistema PNT quais os parâmetros que considera fulcrais para cumprir com os requisitos / necessidades do seu serviço? (As definições de cada termo estão de acordo com a Resolução A.915(22) da IMO.) *

- [ ] Precisão (The accuracy of a measurement or a position with respect to random errors.)
- [ ] Exactidão (The degree of conformance between the estimated or measured parameter of a craft at a given time and i
- [ ] Disponibilidade (The percentage of time that an aid, or system of aids, is performing a required function under stated
- [ ] Integridade (The ability to provide users with warnings within a specified time when the system should not be used fo
- [ ] Cobertura (The coverage provided by a radionavigation system is that surface area or space volume in which the sign
- [ ] Custo reduzido (aquisição, manutenção e actualização)
- [ ] Fiabilidade (A measure of the effectiveness with which gross errors may be detected.)
- [ ] Continuidade (The probability that, assuming a fault-free receiver, a user will be able to determine position with specifi
- [ ] Redundância (The existence of multiple equipment or means for accomplishing a given function in order to increase t
- [ ] Other...

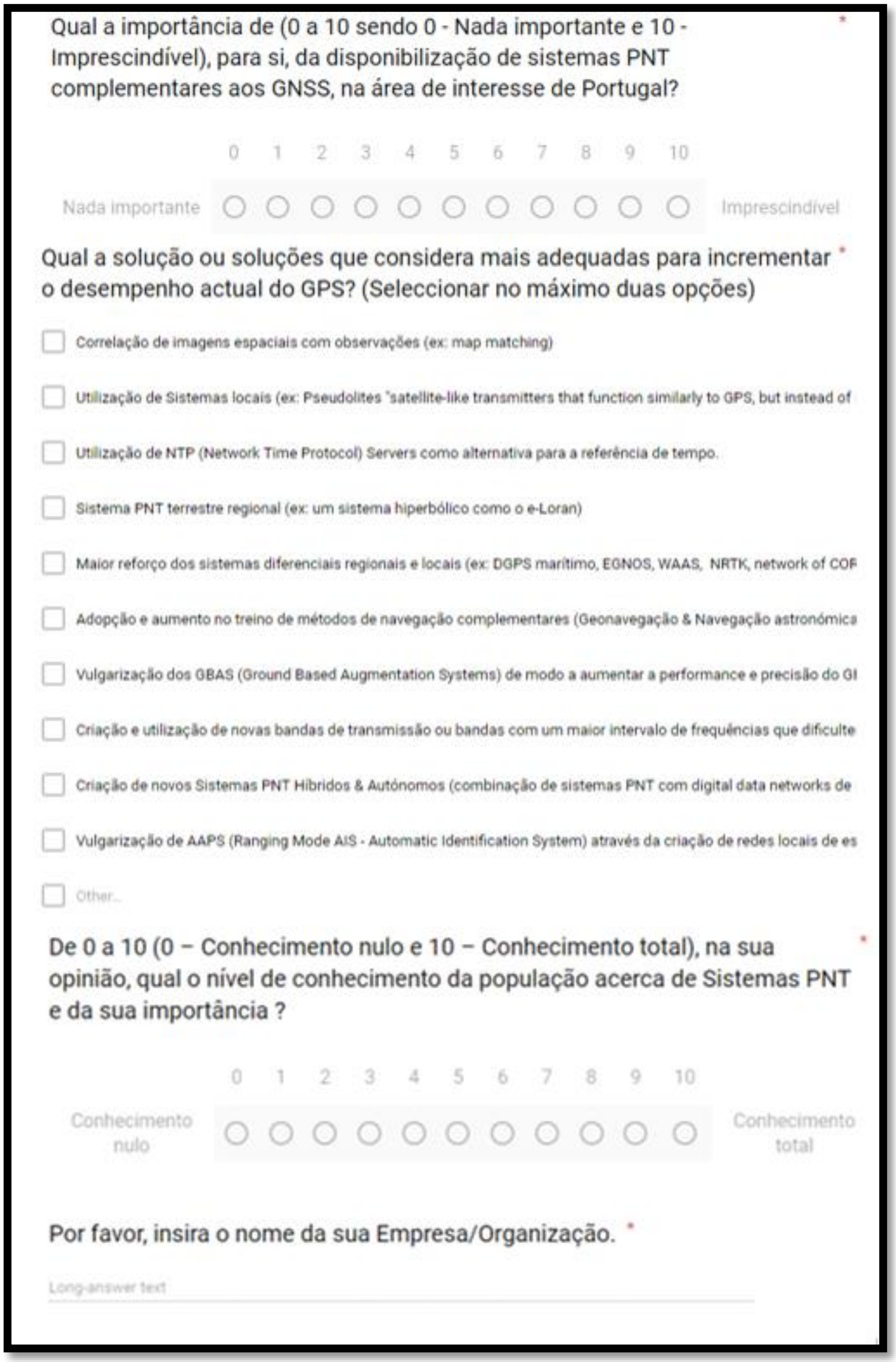
Quais os GNSS ou Sistemas regionais que utiliza/utilizou ou trabalha/trabalhou com? *

- [ ] GPS
- [ ] DGPS
- [ ] WAAS
- [ ] EGNOS
- [ ] GALILEO
- [ ] GLONASS
- [ ] BeiDou
- [ ] IRNSS
- [ ] DORIS
- [ ] Other...

De 0 a 10 (sendo 0-Nada dependente e 10-Completamente dependente) como classifica, na realização do seu serviço, a sua dependência dos GNSS? *

	0	1	2	3	4	5	6	7	8	9	10	
Nada dependente	○	○	○	○	○	○	○	○	○	○	○	Completamente dependente

Figure 29 - Questionnaire (page 4)



Qual a importância de (0 a 10 sendo 0 - Nada importante e 10 - Imprescindível), para si, da disponibilização de sistemas PNT complementares aos GNSS, na área de interesse de Portugal? *

0 1 2 3 4 5 6 7 8 9 10

Nada importante ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ Imprescindível

Qual a solução ou soluções que considera mais adequadas para incrementar o desempenho actual do GPS? (Seleccionar no máximo duas opções) *

- [ ] Correlação de imagens espaciais com observações (ex: map matching)
- [ ] Utilização de Sistemas locais (ex: Pseudolites "satellite-like transmitters that function similarly to GPS, but instead of
- [ ] Utilização de NTP (Network Time Protocol) Servers como alternativa para a referência de tempo.
- [ ] Sistema PNT terrestre regional (ex: um sistema hiperbólico como o e-Loran)
- [ ] Maior reforço dos sistemas diferenciais regionais e locais (ex: DGPS marítimo, EGNOS, WAAS, NRTK, network of COR
- [ ] Adopção e aumento no treino de métodos de navegação complementares (Geonavegação & Navegação astronómica
- [ ] Vulgarização dos GBAS (Ground Based Augmentation Systems) de modo a aumentar a performance e precisão do GI
- [ ] Criação e utilização de novas bandas de transmissão ou bandas com um maior intervalo de frequências que dificulte
- [ ] Criação de novos Sistemas PNT Hibridos & Autónomos (combinação de sistemas PNT com digital data networks de
- [ ] Vulgarização de AAPS (Ranging Mode AIS - Automatic Identification System) através da criação de redes locais de es
- [ ] Other...

De 0 a 10 (0 – Conhecimento nulo e 10 – Conhecimento total), na sua opinião, qual o nível de conhecimento da população acerca de Sistemas PNT e da sua importância ? *

0 1 2 3 4 5 6 7 8 9 10

Conhecimento nulo ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ Conhecimento total

Por favor, insira o nome da sua Empresa/Organização. *

Long-answer text

Figure 30 - Questionnaire (page 5)

APPENDIX C

Description: This Appendix shows the graphs (made through Microsoft Excel) that were made according to the Online Questionnaire data.

Figure 31 - Open interview analysis (Users - Time)

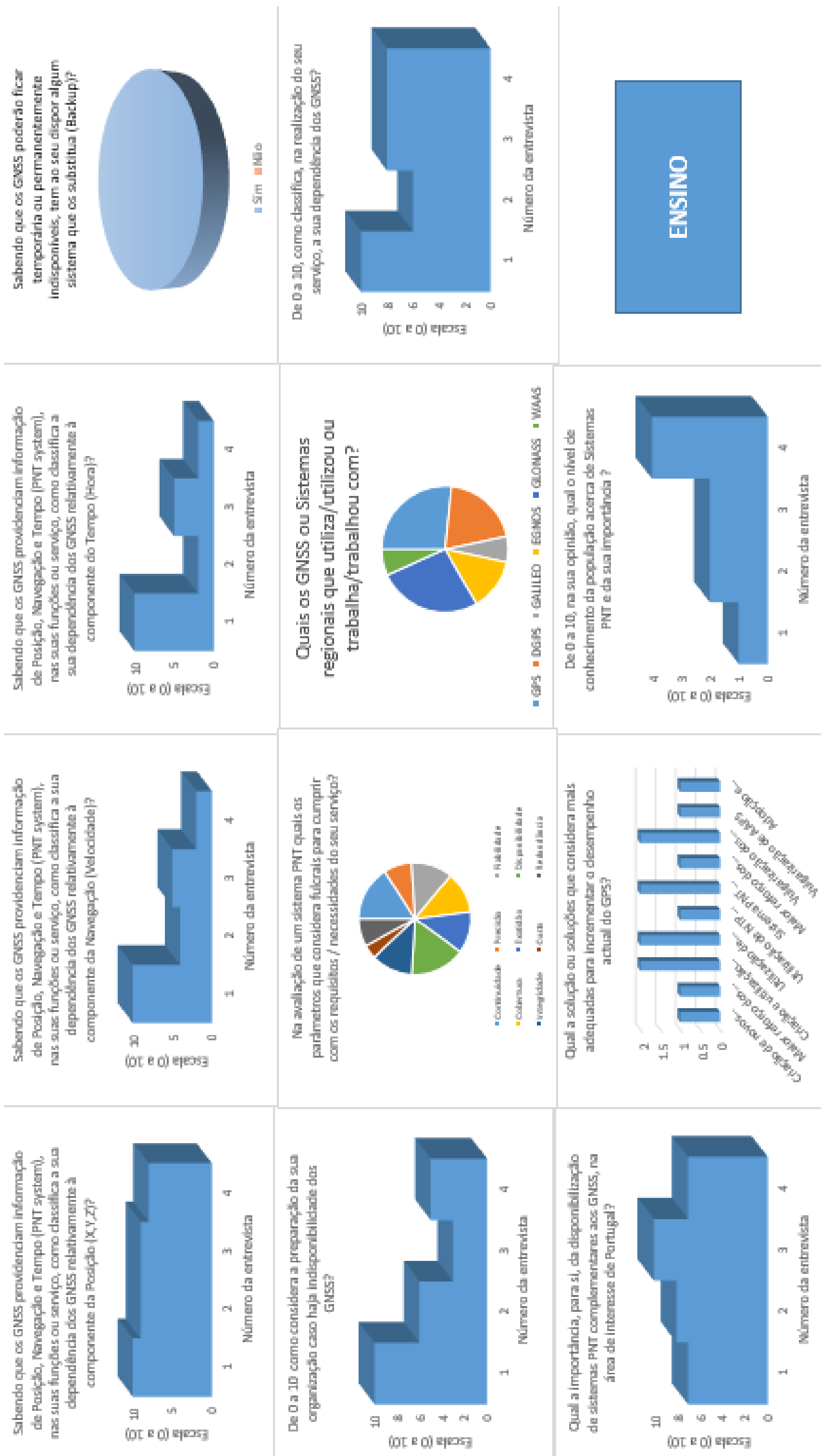


Figure 32 - Open interview analysis (Academia)

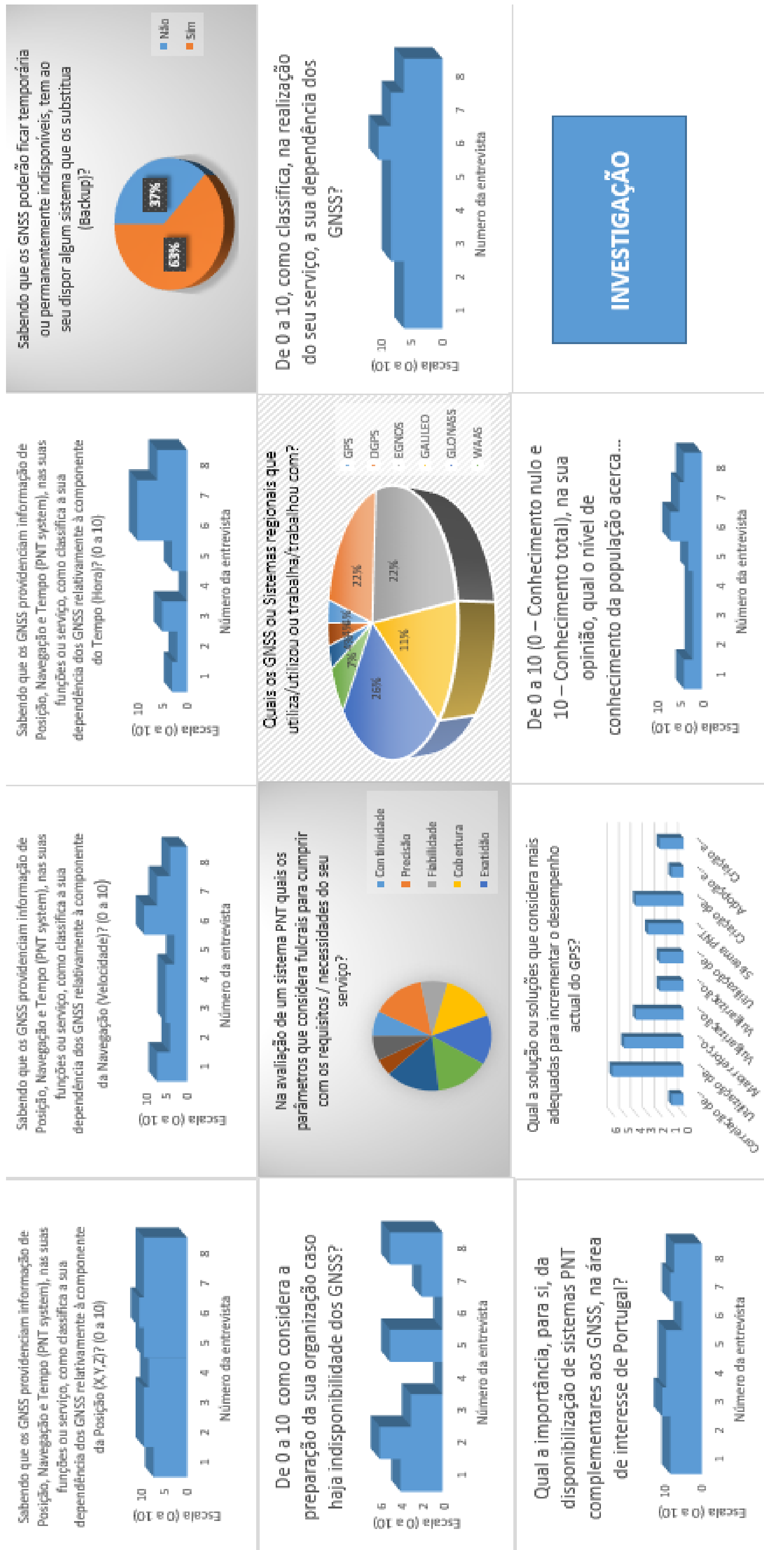


Figure 33 - Open interview analysis (Investigation)

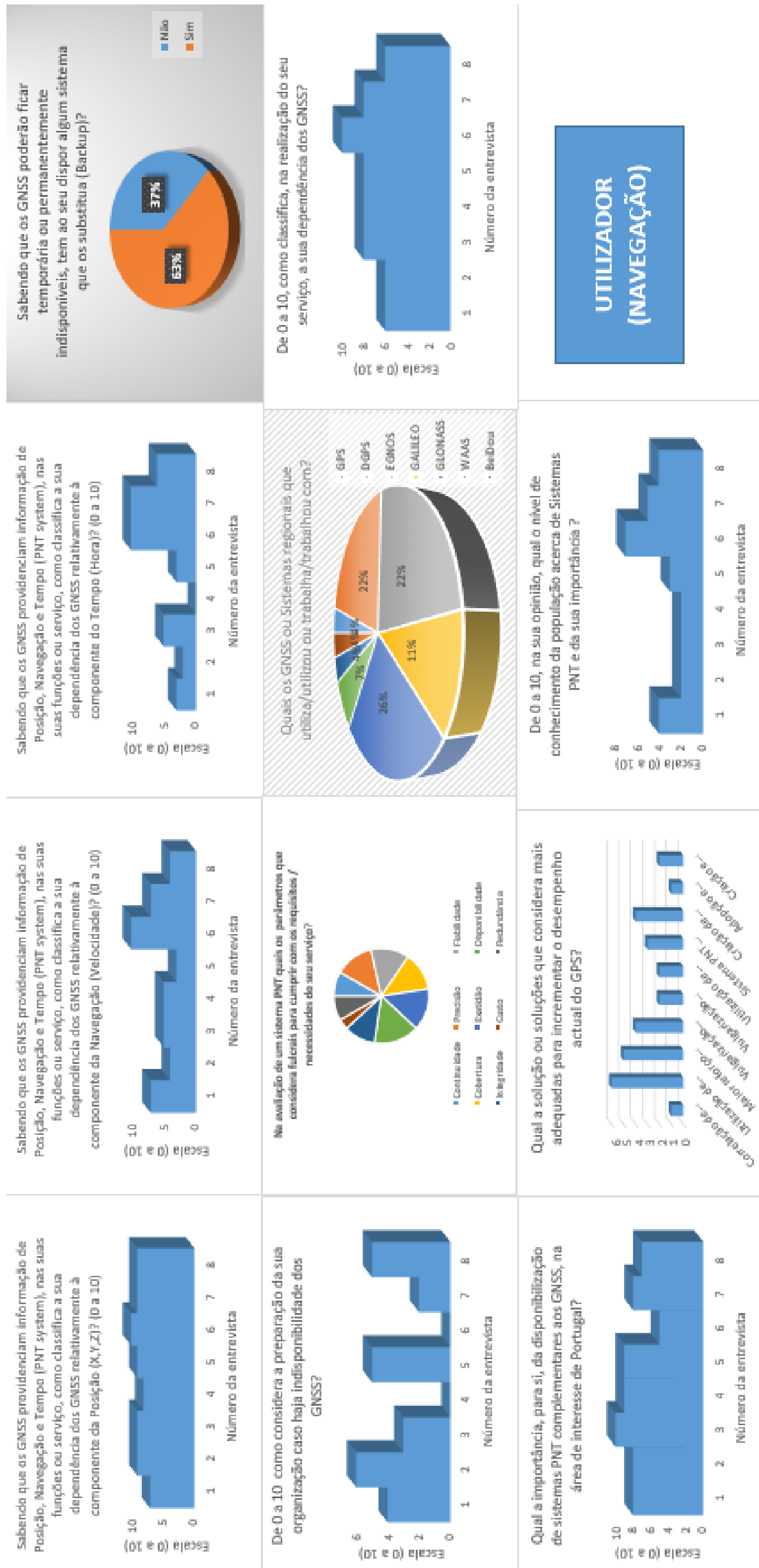


Figure 34 - Open interview analysis (Users - Navigation)

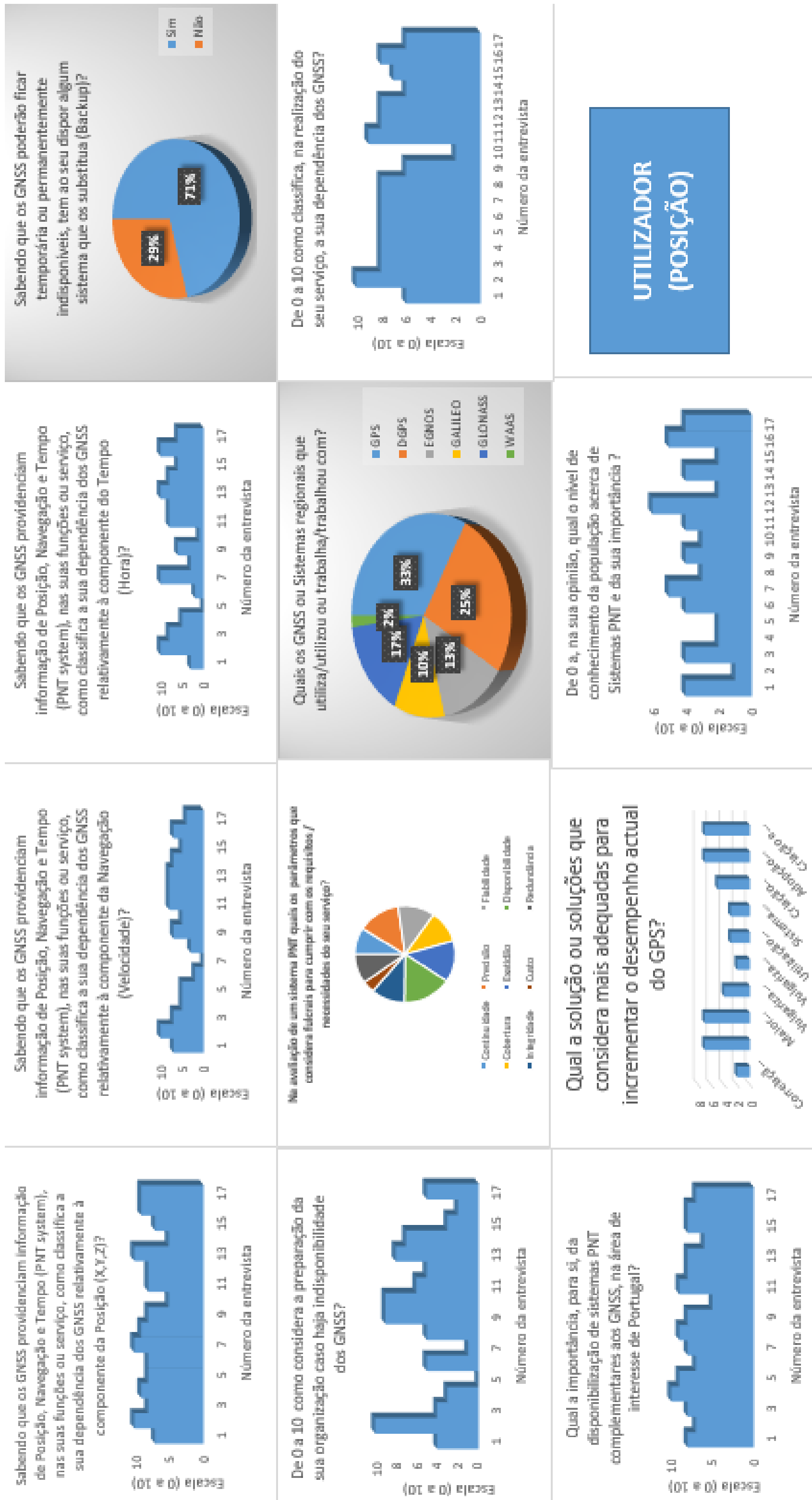


Figure 35 - Open interview analysis (Users - Positioning)

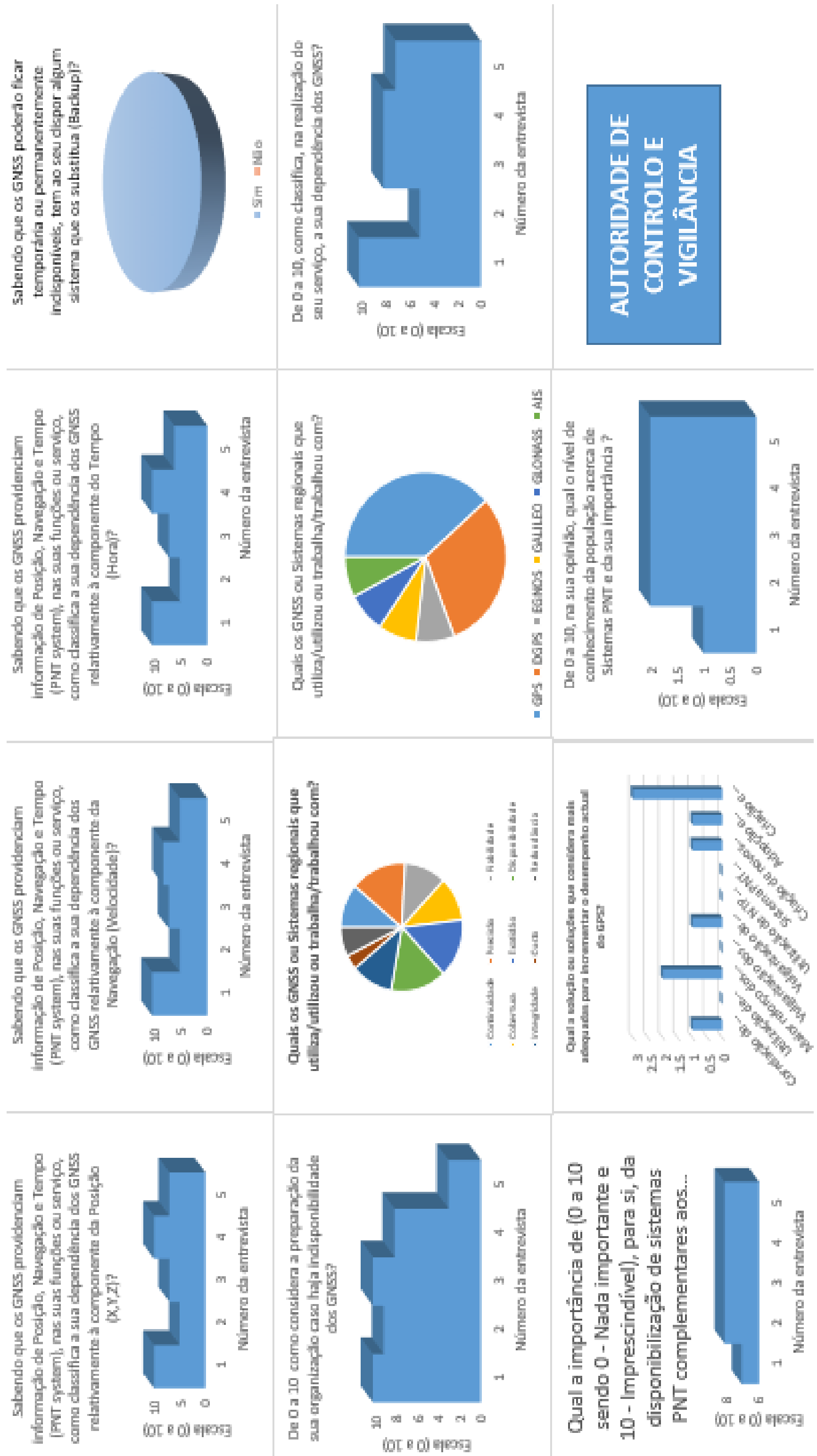


Figure 36 - Open interview analysis (Control & Vigilance Authorities)

Figure 37 - Open interview analysis (GNSS-depend services supplier)

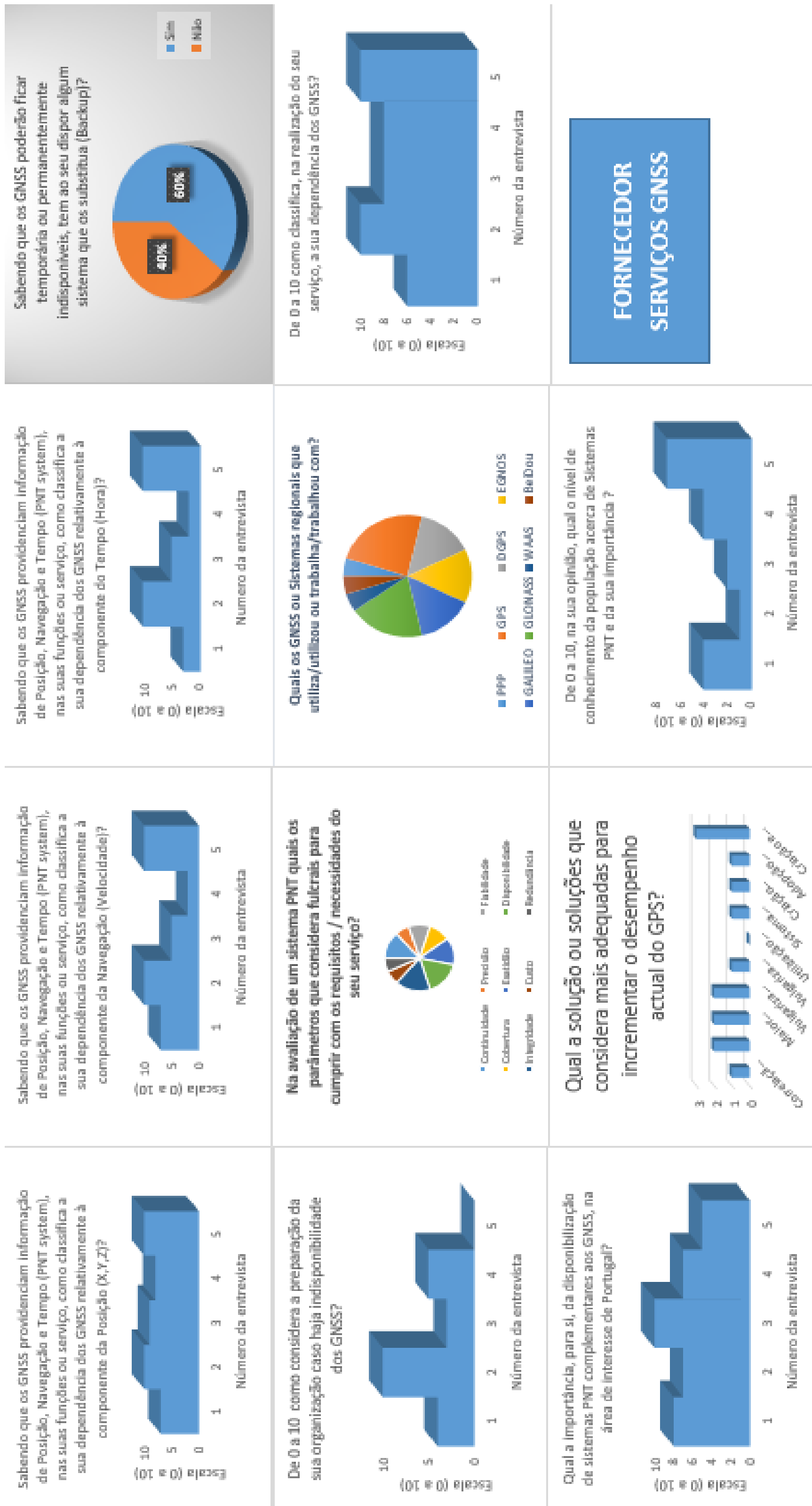


Figure 38 - Open interview analysis (GNSS services supplier)

APPENDIX D

Description: This Appendix shows the Personal Interview that was answered by all the interested PNT Stakeholders.

Entrevista Pessoal

- De que maneira é que a sua função/serviço se interliga ou depende de GNSS?
- Em caso de ocorrer uma falha total, temporária ou permanente, dos GNSS dos quais o seu serviço depende, quais são as alternativas que dispõe para a realização das suas funções e, consequentemente, o funcionamento normal da sua organização?
- Na sua opinião como é que em Portugal se deveria abordar esta problemática / vulnerabilidade?

Figure 39 - Personal interview

APPENDIX E

Description: This Appendix presents a Mind Map for the results of the Personal Interviews, according to the topics that emerged from the interviews analysis, after several iterations of the coding process.

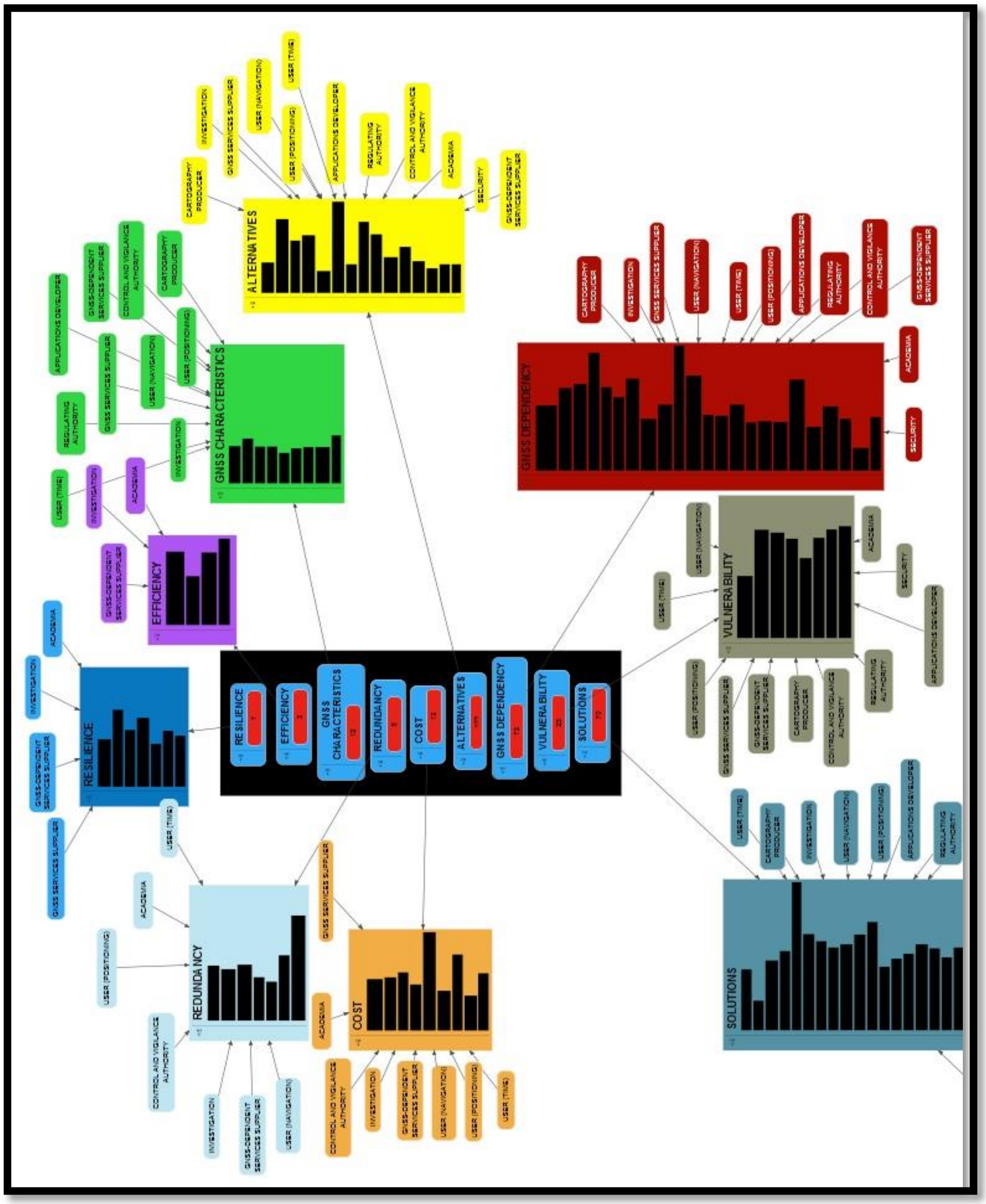


Figure 40 - Common topics (1)

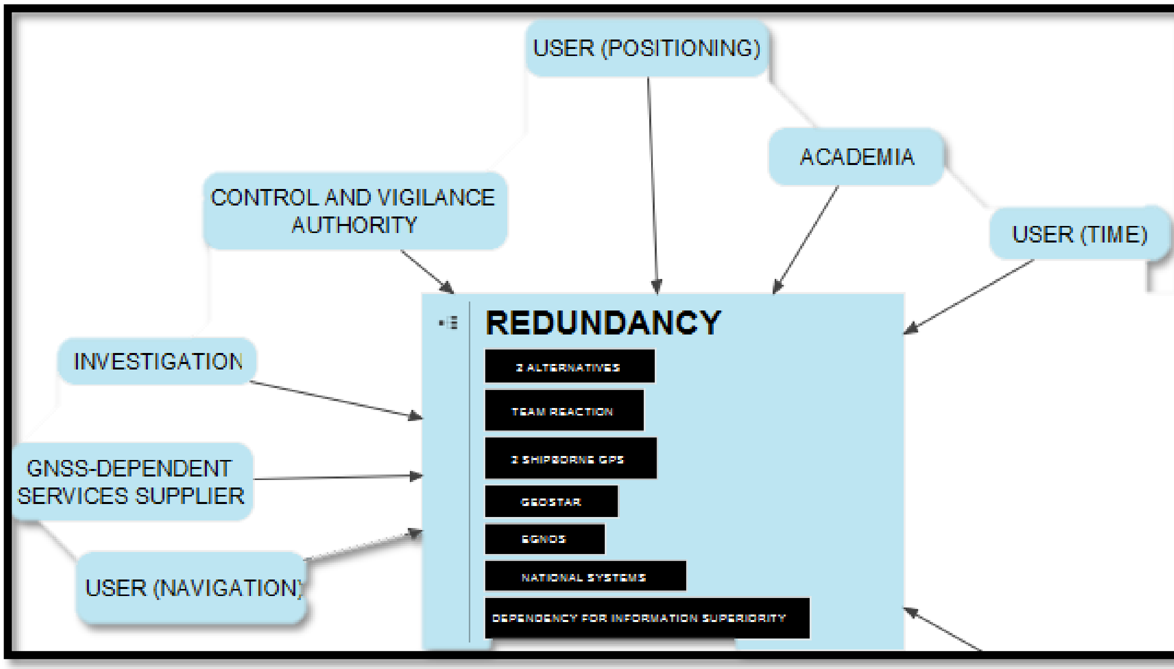


Figure 41 - Common topics (2)

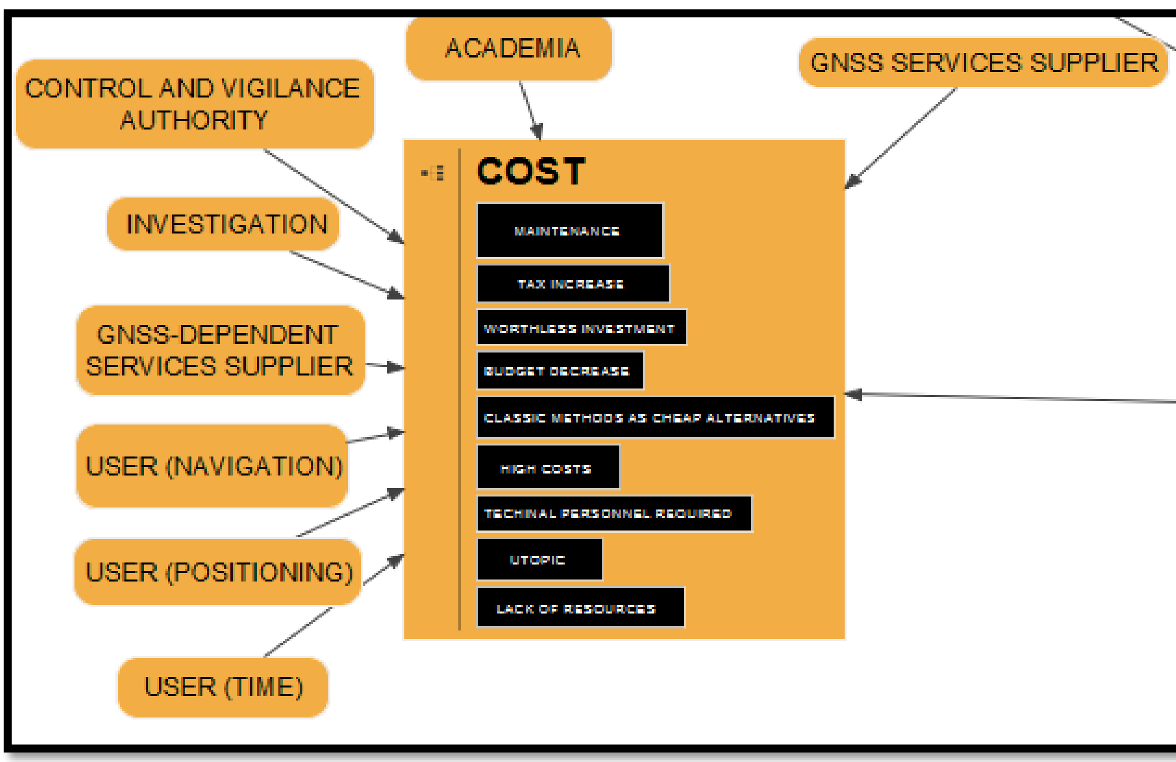


Figure 42 - Common topics (3)

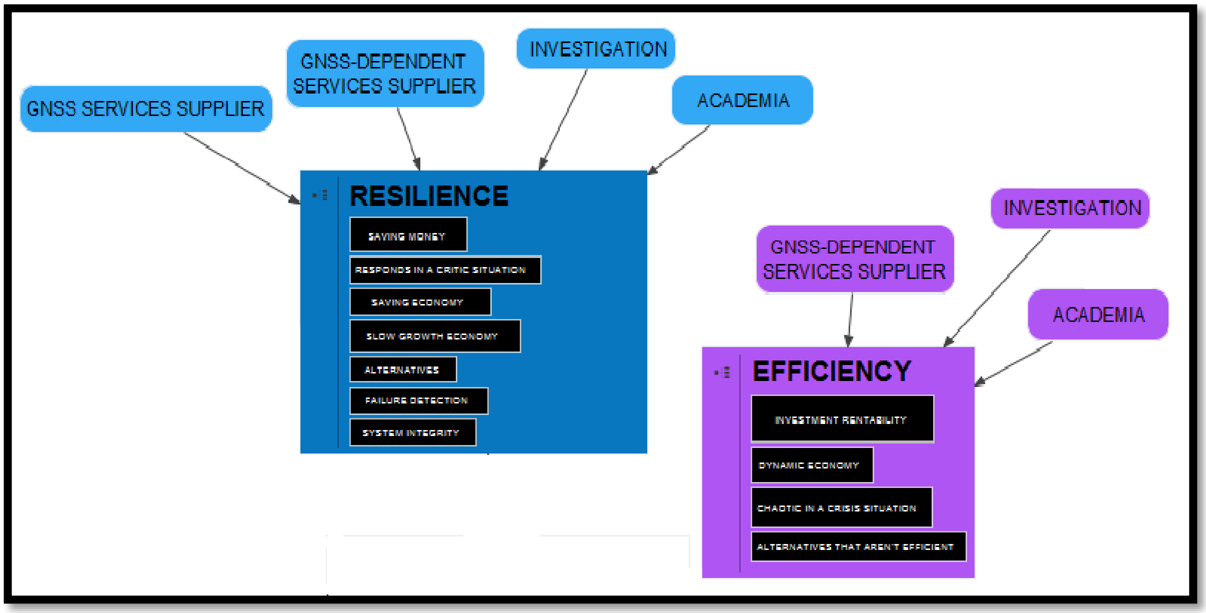


Figure 43 - Common topics (4)

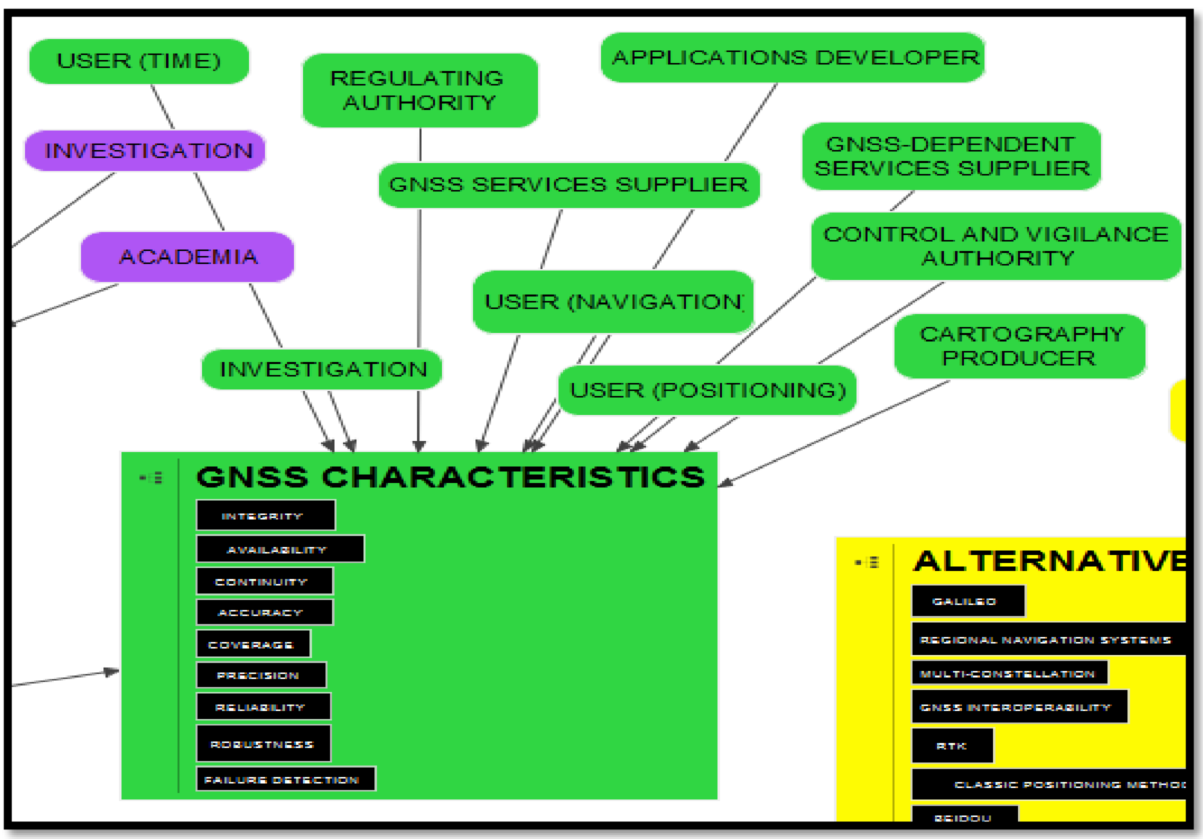


Figure 44 - Common topics (5)

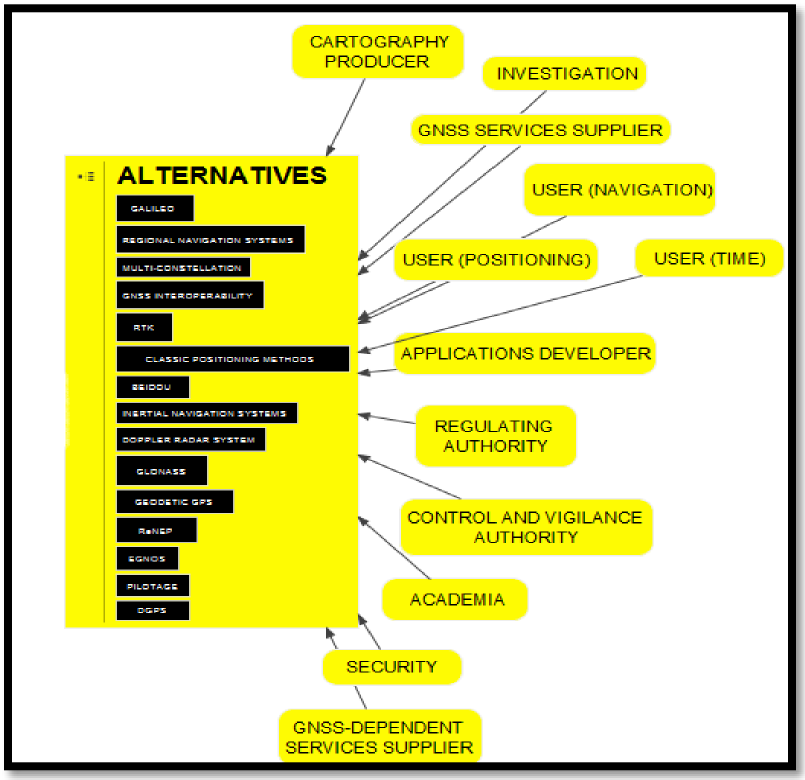


Figure 45 - Common topics (6)

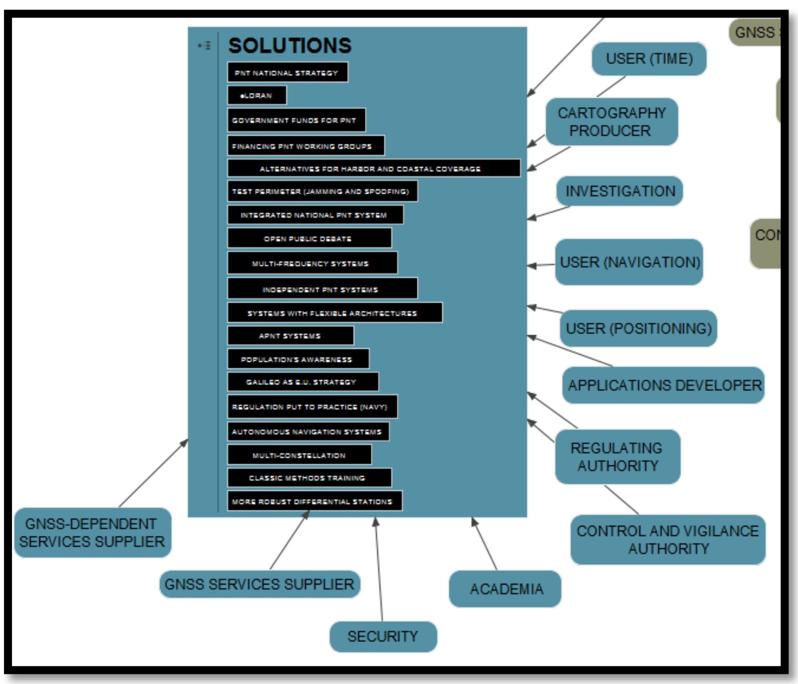


Figure 46 - Common topics (7)

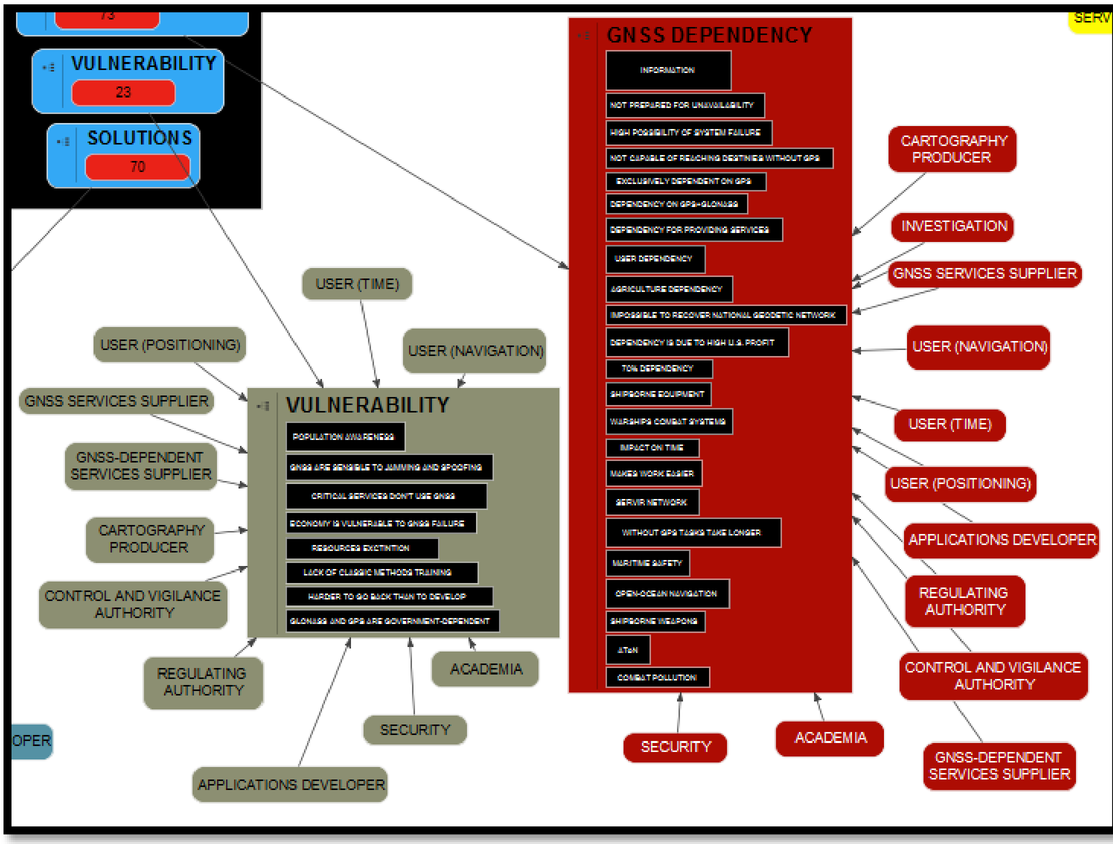


Figure 47 - Common topics (8)

APPENDIX F

Description: This Appendix shows a Mind Map based on the results of the Personal Interviews (which Stakeholders referred each topic and how many of them did).

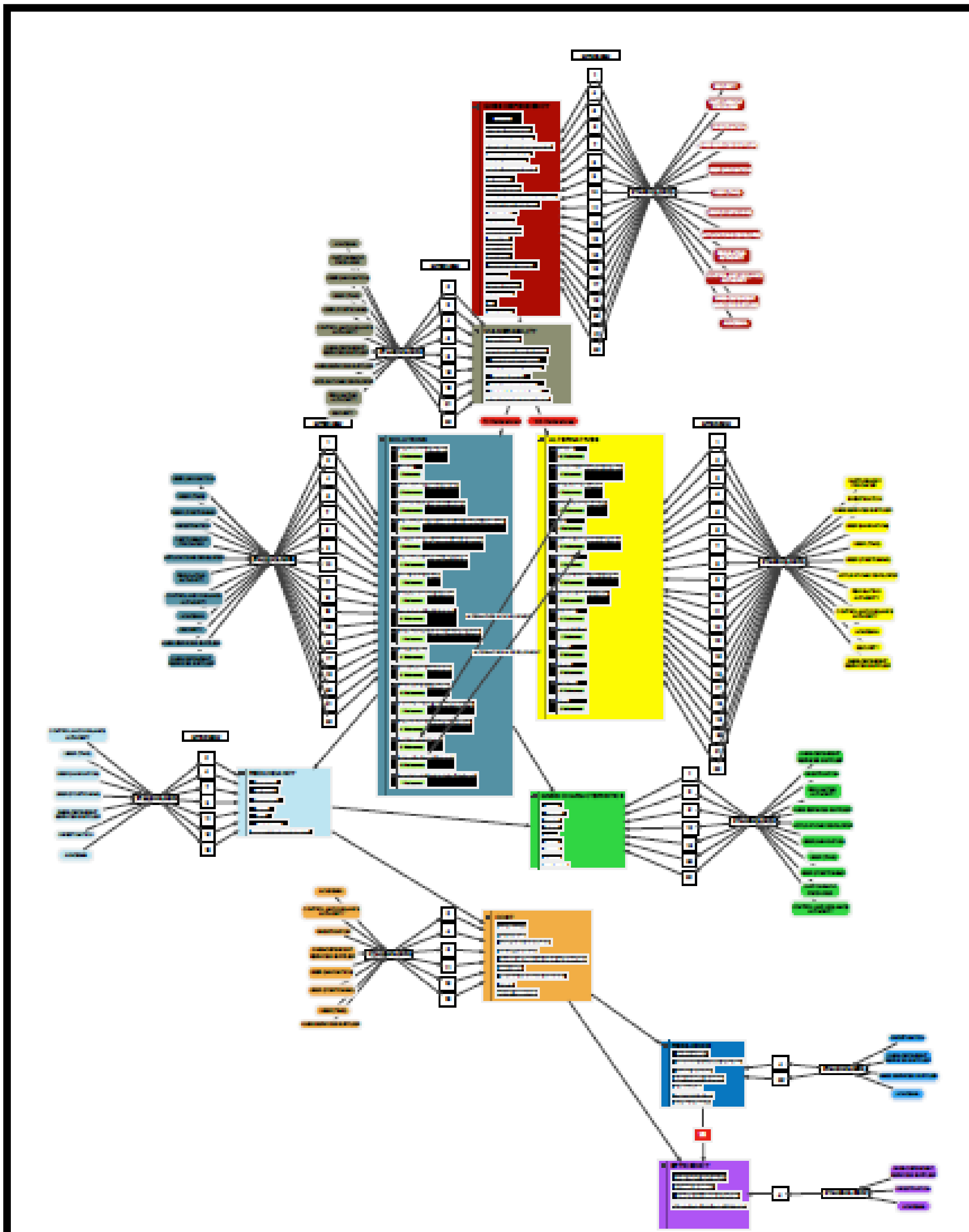


Figure 48 - Personal interview results (1)

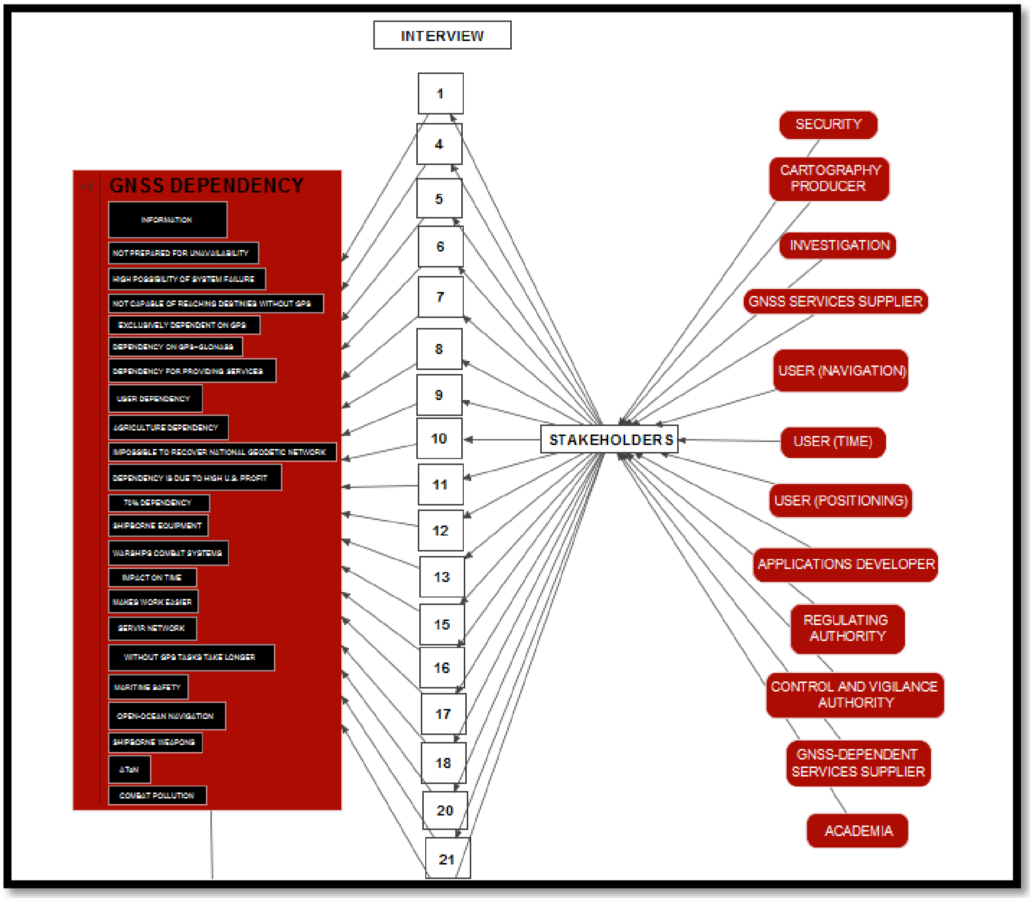


Figure 49 - Personal interview results (2)

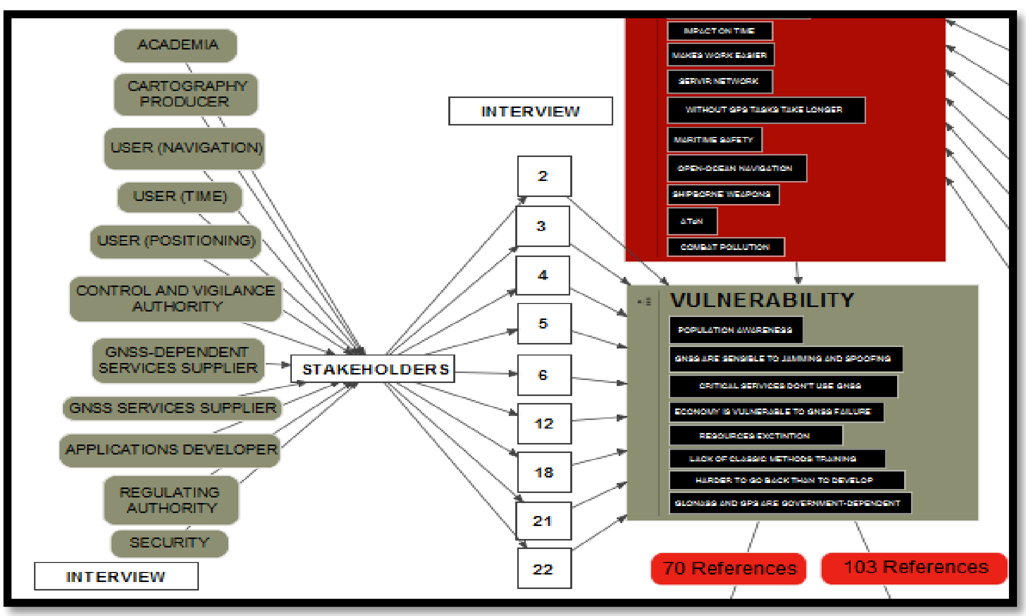


Figure 50 - Personal interview results (3)

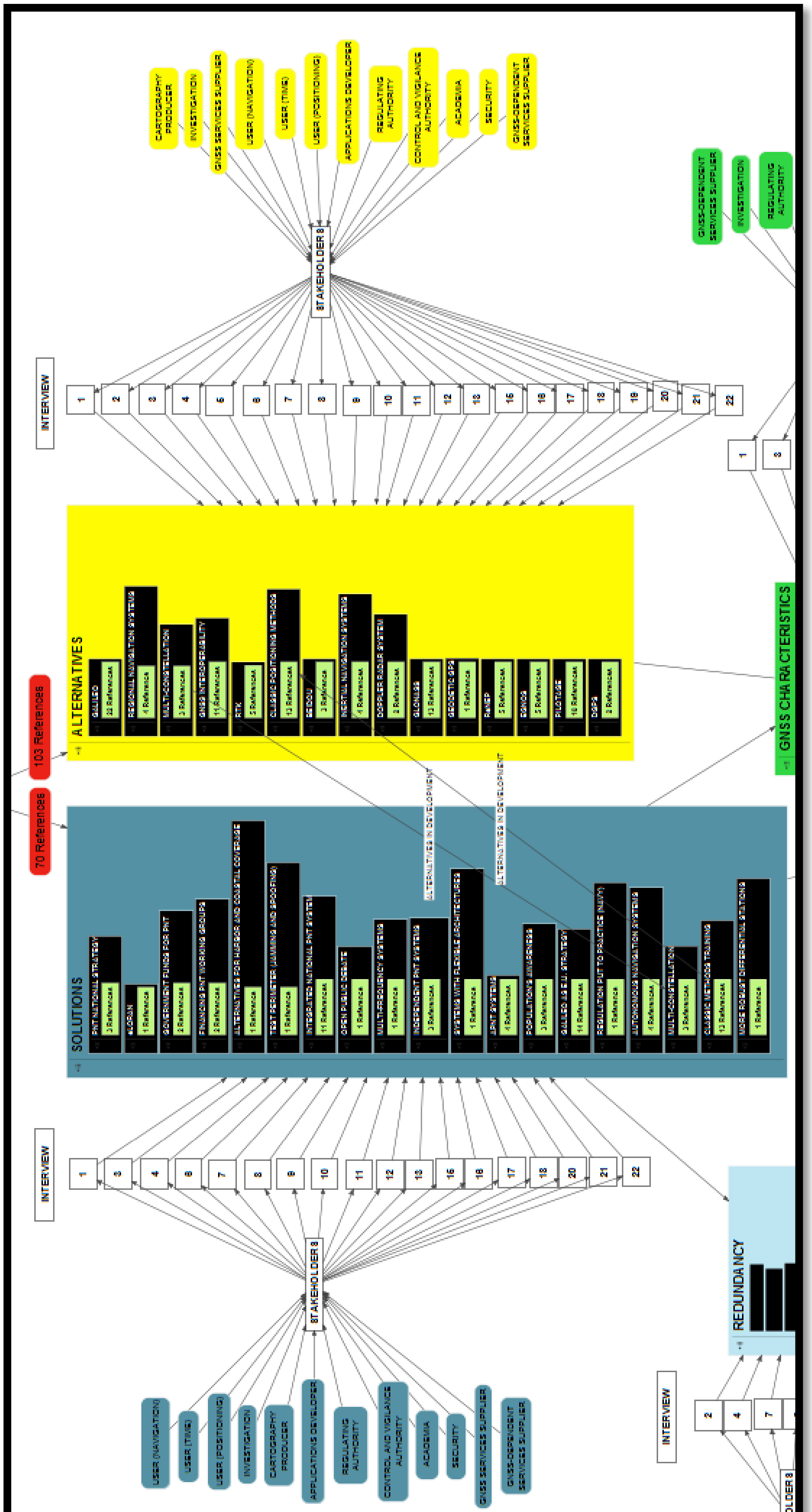


Figure 51 - Personal interview results (4)

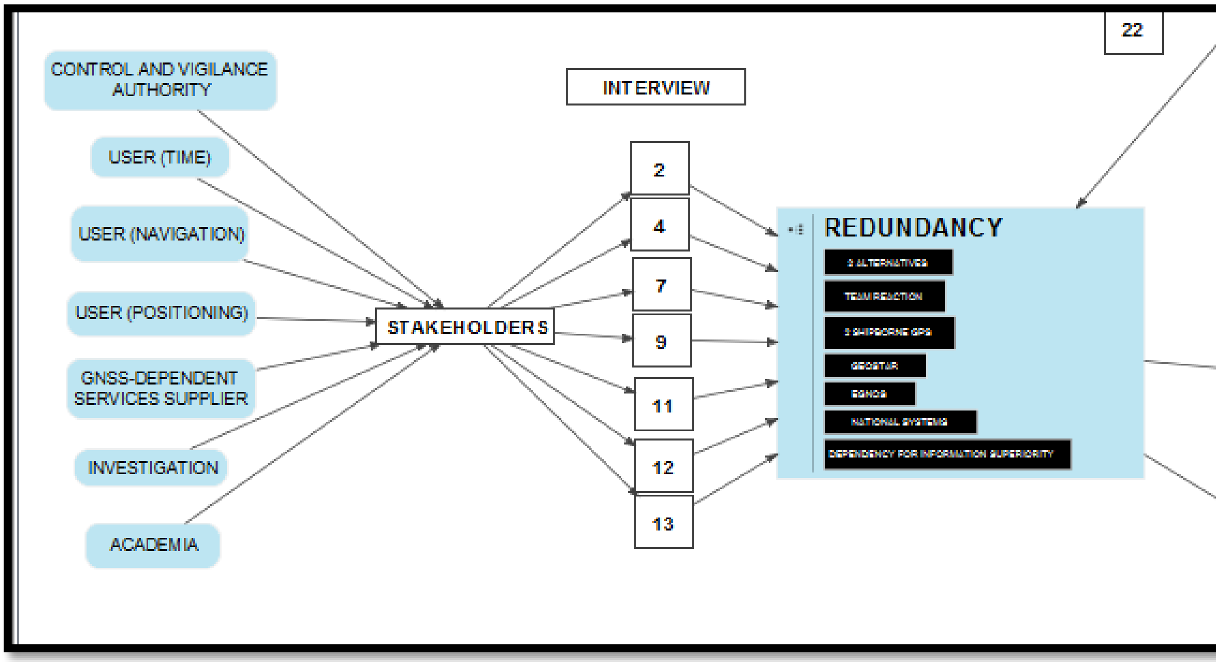


Figure 52 - Personal interview results (5)

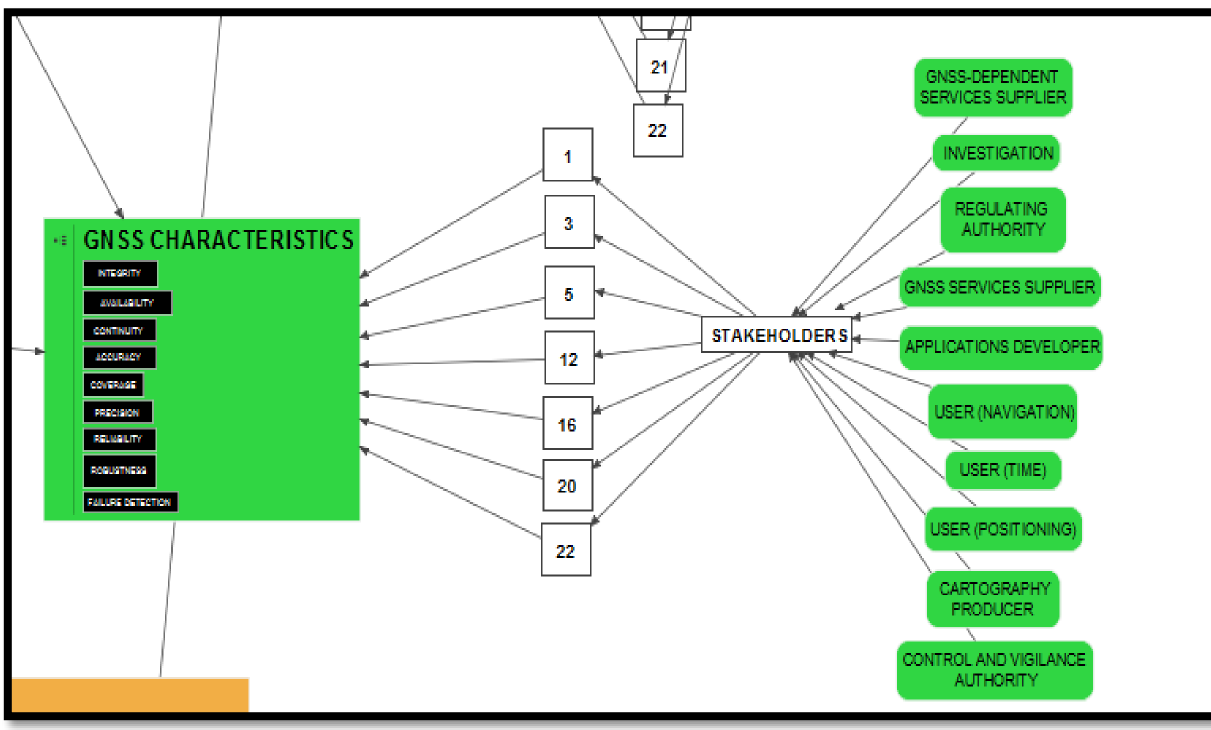


Figure 53 - Personal interview results (6)

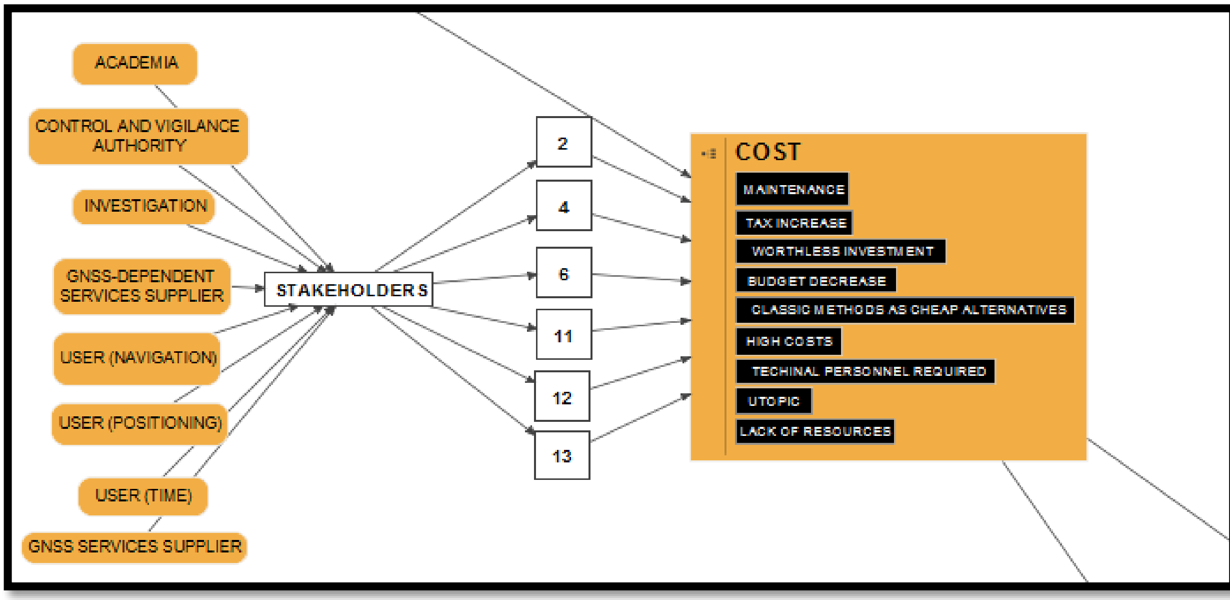


Figure 54 - Personal interview results (7)

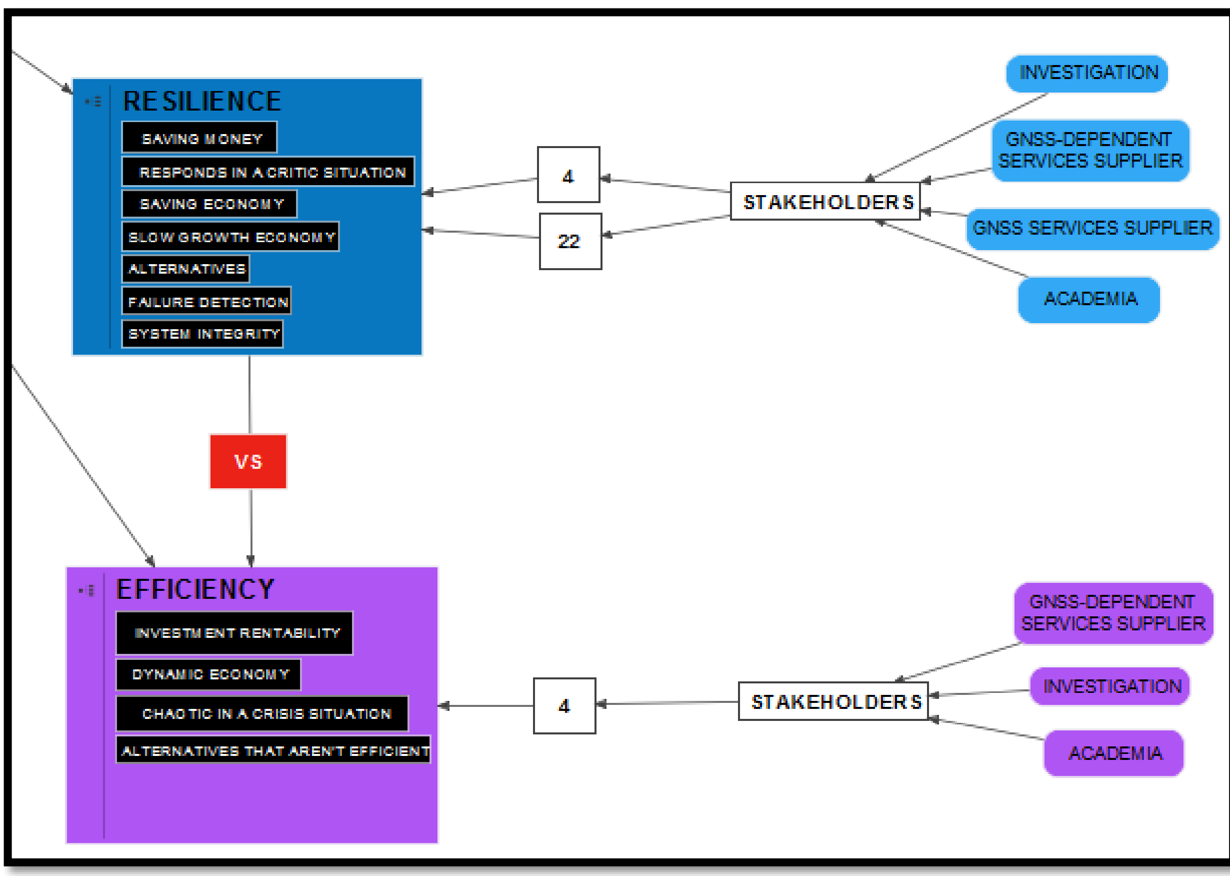


Figure 55 - Personal interview results (8)

APPENDIX G

Description: This Appendix shows pictures of the Jamming Trials aboard a Portuguese Navy Warship.

Figure 56 - R&S FSH3 Antenna

Figure 57 - Trial equipment (R&S FSH3)

Figure 58 - Putty program

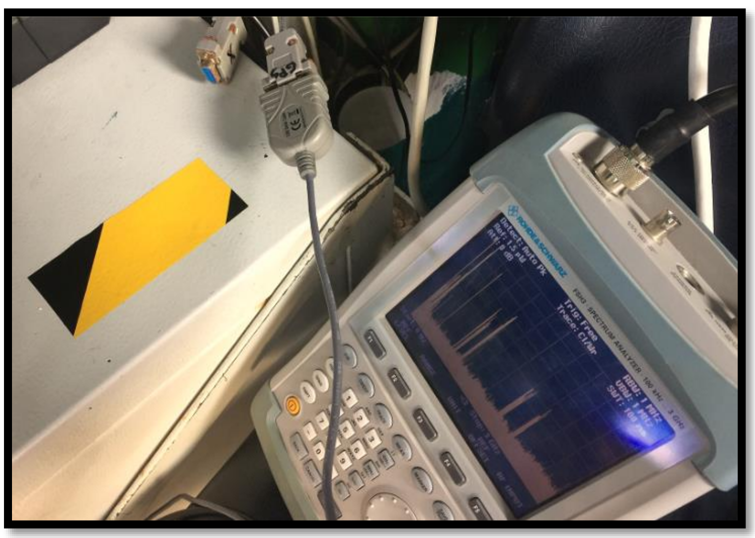


Figure 59 - R&S FSH3

Figure 60 - AIS "no sensor position"

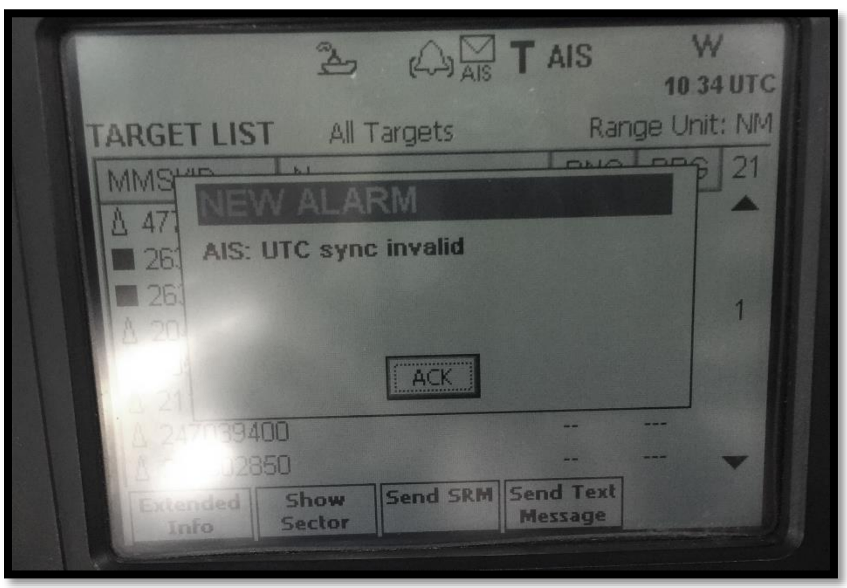


Figure 61 - AIS "UTC sync invalid"

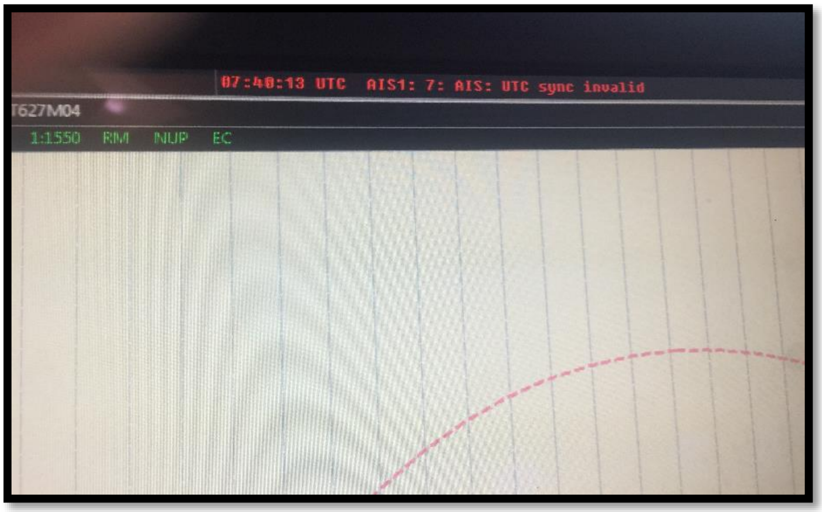


Figure 62 - ECDIS (AIS alarm)

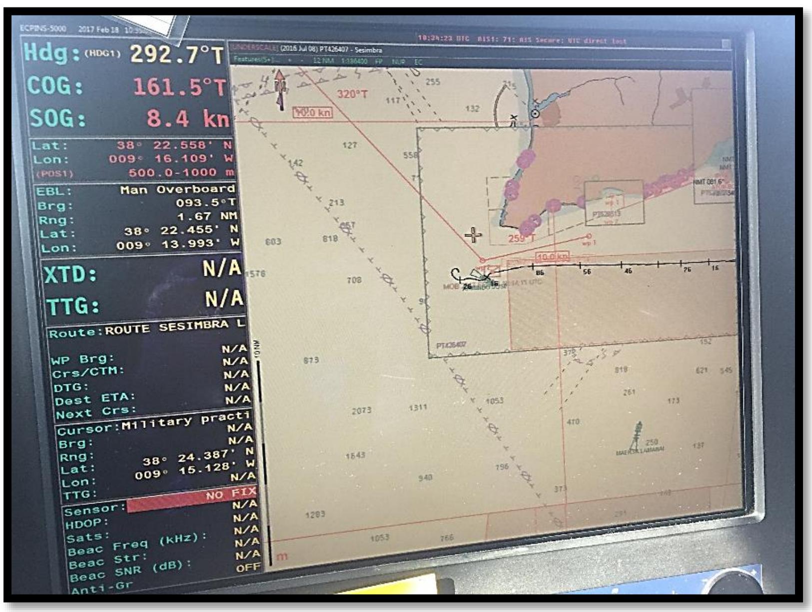


Figure 63 - ECDIS (No fix)

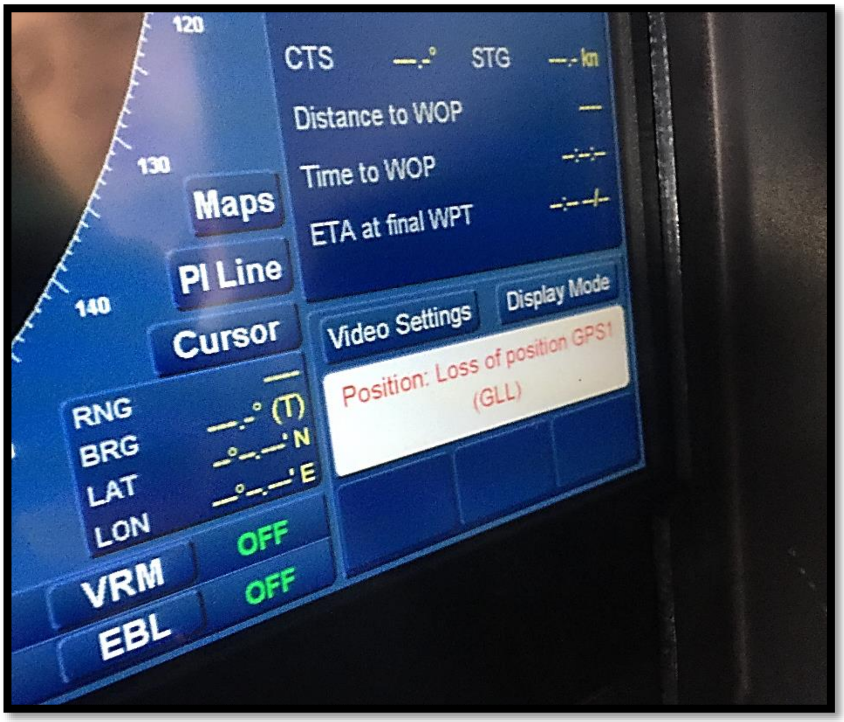


Figure 64 - Radar KH1007 (loss of position)

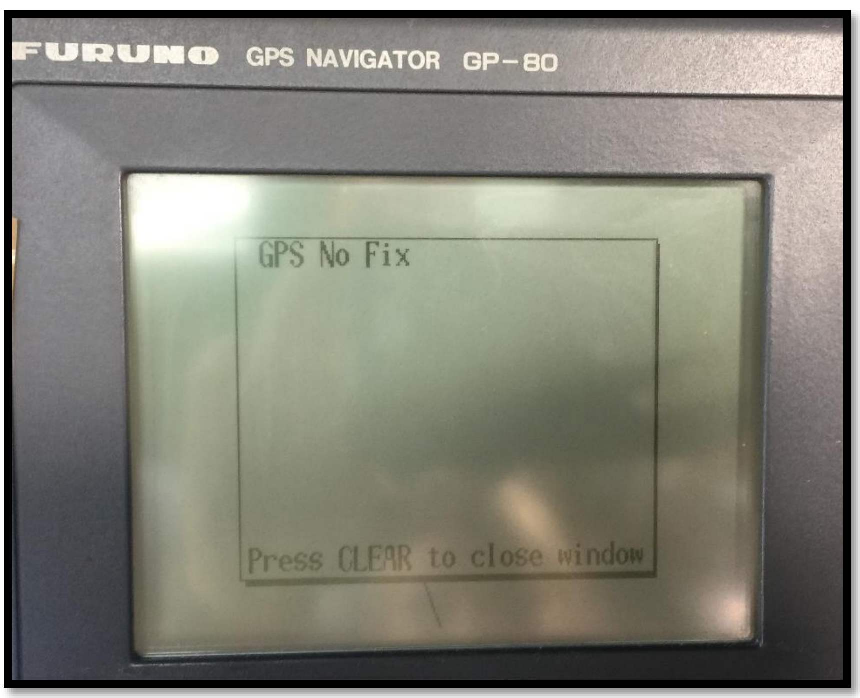


Figure 65 - GPS Furuno - no fix

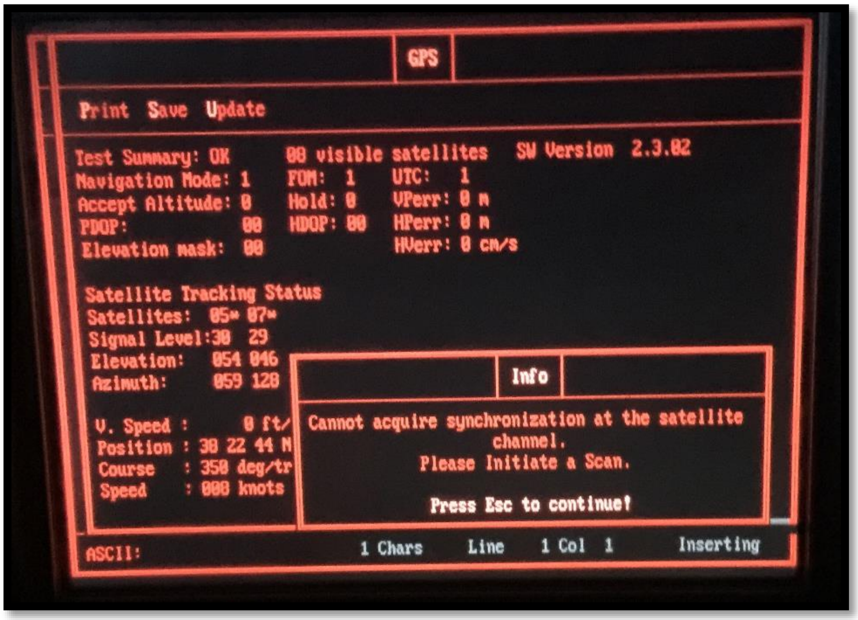


Figure 66 - VHF sailor (no satellite sync)

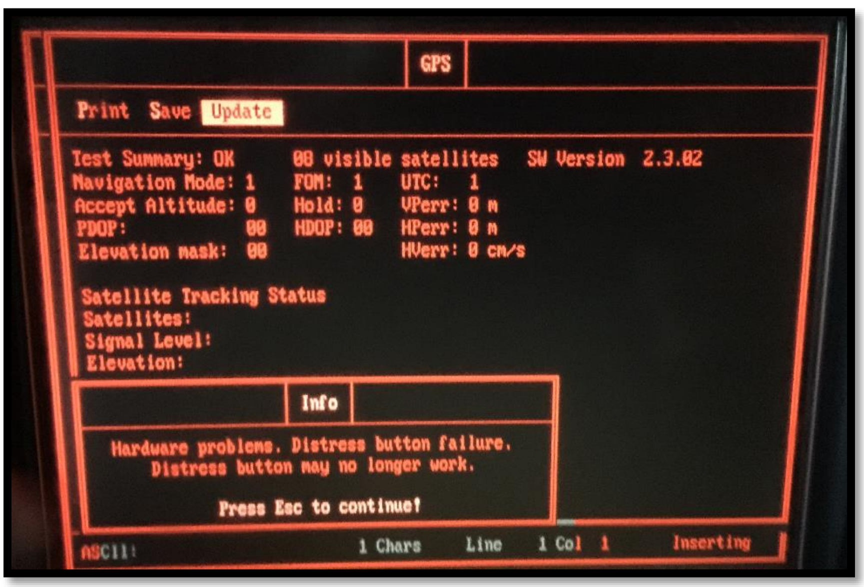
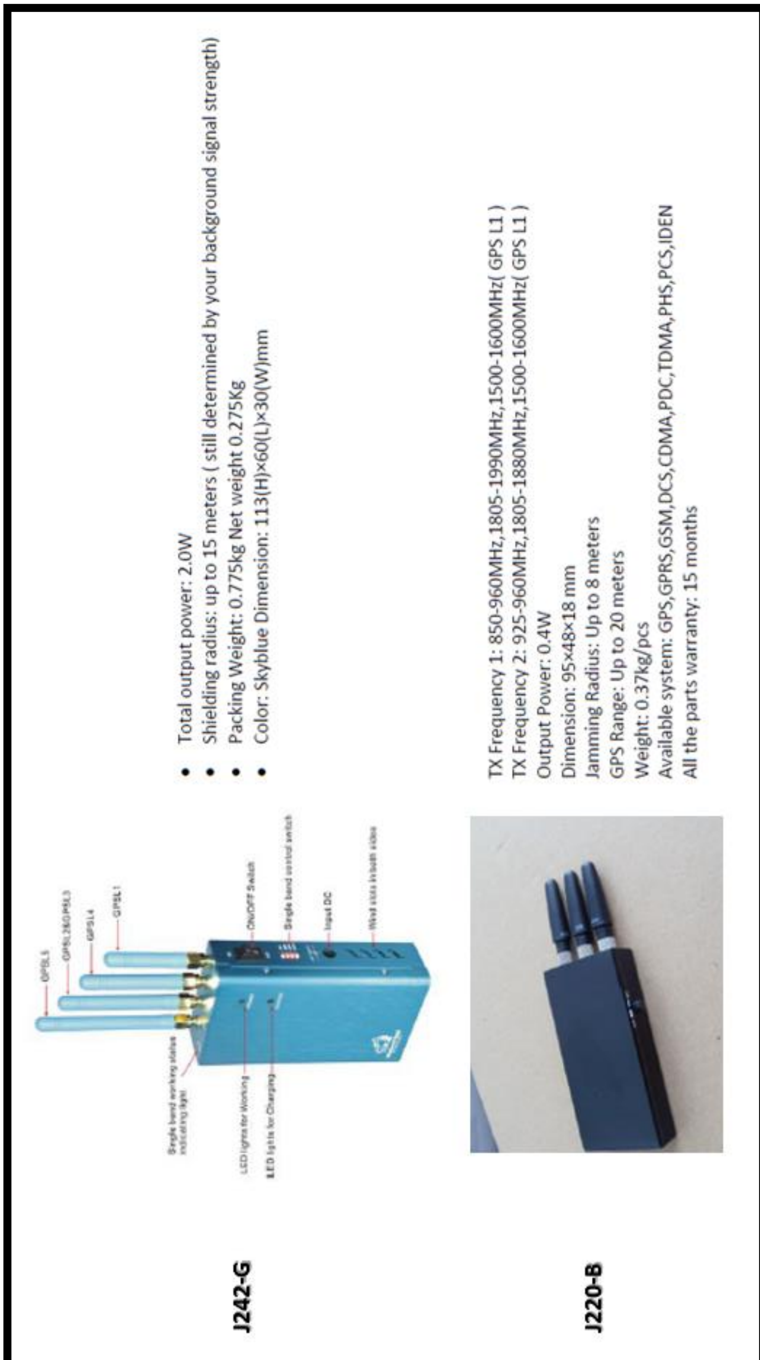


Figure 67 - VHF sailor (distress failure)

APPENDIX H

Description: This Appendix shows the Technical description of both Jammers used (J242-G and J220-B).



J242-G

- Total output power: 2.0W
- Shielding radius: up to 15 meters (still determined by your background signal strength)
- Packing Weight: 0.775kg Net weight 0.275Kg
- Color: Skyblue Dimension: 113(H)×60(L)×30(W)mm

J220-B

TX Frequency 1: 850-960MHz,1805-1990MHz,1500-1600MHz(GPS L1)
TX Frequency 2: 925-960MHz,1805-1880MHz,1500-1600MHz(GPS L1)
Output Power: 0.4W
Dimension: 95×48×18 mm
Jamming Radius: Up to 8 meters
GPS Range: Up to 20 meters
Weight: 0.37kg/pcs
Available system: GPS,GPRS,GSM,DCS,CDMA,PDC,TDMA,PHS,PCS,IDEN
All the parts warranty: 15 months

APPENDIX I

Description: This Appendix shows the illustrative representation of the path for a resilient PNT system in Portugal.